VNNIC Internet for all

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM INTERNET VIỆT NAM

IPv6 VIETNAM

IPv6 TOÀN TẬP

LÀM CHỦ GIAO THỨC INTERNET THẾ HỆ MỚI

IC PUBLISHER
NHÀ XUẤT BẢN THÔNG TIN VÀ TRUYỀN THÔNG

VNNIC
Internet for all

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM INTERNET VIỆT NAM

IPv6 VIETNAM

IPv6 TOÀN TẬP

LÀM CHỦ GIAO THỨC INTERNET THẾ HỆ MỚI

IC PUBLISHER
NHÀ XUẤT BẢN THÔNG TIN VÀ TRUYỀN THÔNG

CHỈ ĐẠO BIÊN SOẠN

ÔNG NGUYỄN HỒNG THẮNG
Giám đốc, Trung tâm Internet Việt Nam

NHÓM BIÊN SOẠN

NGUYỄN VĂN BÌNH (Chủ biên)
NGUYỄN TRƯỜNG GIANG / HOÀNG XUÂN HIẾU
NGUYỄN THỊ THU THỦY / NGUYỄN THỊ OANH

CHỊU TRÁCH NHIỆM XUẤT BẢN, NỘI DUNG

TS. TRẦN CHÍ ĐẠT
Giám đốc – Tổng biên tập

Chịu trách nhiệm bản thảo

BÀ NGÔ THỊ MỸ HẠNH
Phó Giám đốc – Phó Tổng Biên tập

Biên tập nội dung:

NGUYỄN LONG BIÊN / VŨ THỊ NGỌC MAI

Trình bày, thiết kế sách:

NGUYỄN NGỌC MẠNH

Biên tập sách điện tử:

NGUYỄN TIẾN PHÁT

Trình bày sách điện tử:

NGUYỄN THỊ THẢO

NHÀ XUẤT BẢN THÔNG TIN VÀ TRUYỀN THÔNG

Trụ sở: Tầng 6, Tòa nhà Cục Tần số vô tuyến điện
115 Trần Duy Hưng, quận Cầu Giấy, TP. Hà Nội
ĐT Biên tập: 024.35772143; ĐT Phát hành: 024.35772138
E-mail: nxb.tttt@mst.gov.vn www.nxbthongtintruyenthong.vn; book365.vn; ebook365.vn; ebook.gov.vn
Số XNĐKXB: 2154-2025/CXBIPH/1-86/TTTT
Số QĐXB: 314/QĐ - NXB TTTT ngày 13 tháng 6 năm 2025
Mã ISBN: 978-604-45-1147-4
In xong và nộp lưu chiểu Quý II năm 2025

LỜI MỞ ĐẦU

Bạn có biết, mỗi giây trôi qua, hàng triệu thiết bị mới được kết nối vào mạng Internet, nhưng không gian địa chỉ IPv4 đã không còn đủ để đáp ứng làn sóng bùng nổ này. IPv6 là chìa khóa mở ra tương lai của một Internet lớn hơn, an toàn hơn và không giới hạn.

Chúng ta đang sống trong kỷ nguyên bùng nổ kết nối, nơi Internet trở thành huyết mạch của nền kinh tế số và cuộc cách mạng công nghiệp 4.0. Giao thức, địa chỉ Internet thế hệ mới IPv6 là giải pháp tất yếu để đáp ứng nhu cầu kết nối ngày càng tăng, hướng đến một hạ tầng Internet hiện đại, linh hoạt và bền vững.

Các sự kiện mang tính lịch sử **"World IPv6 Day"** (2011) và **"World IPv6 Launch"** (2012), những tập đoàn công nghệ như Google, Meta, Akamai đã mở đường cho việc hình thành thế hệ Internet IPv6 mới. Tại Việt Nam, hành trình phát triển IPv6 bắt đầu từ năm 2008 với Chỉ thị số 03/2008/CT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) và sự ra đời của Ban Công tác thúc đẩy phát triển IPv6 quốc gia. Dấu mốc quan trọng tiếp theo là sự kiện khai trương Mạng IPv6 quốc gia **"Viet Nam IPv6 Launch"** vào **"Ngày IPv6 Việt Nam"** năm 2013. Đến cuối năm 2024, tỷ lệ người dùng IPv6 tại Việt Nam đã đạt 65,5%, đưa nước ta vươn lên đứng thứ 7 toàn cầu - minh chứng rõ nét cho tầm nhìn và quyết tâm của Việt Nam trong việc bắt kịp xu thế toàn cầu.

Trong hành trình này, Trung tâm Internet Việt Nam (VNNIC) đóng vai trò nòng cốt – không chỉ trong quản lý tài nguyên Internet mà còn thúc đẩy triển khai IPv6 thông qua đào tạo, hội thảo, qua nền tảng học tập trực tuyến VNNIC Internet Academy (academy.vnnic.vn) và xây dựng năng lực nâng cao cho cộng đồng kỹ thuật.

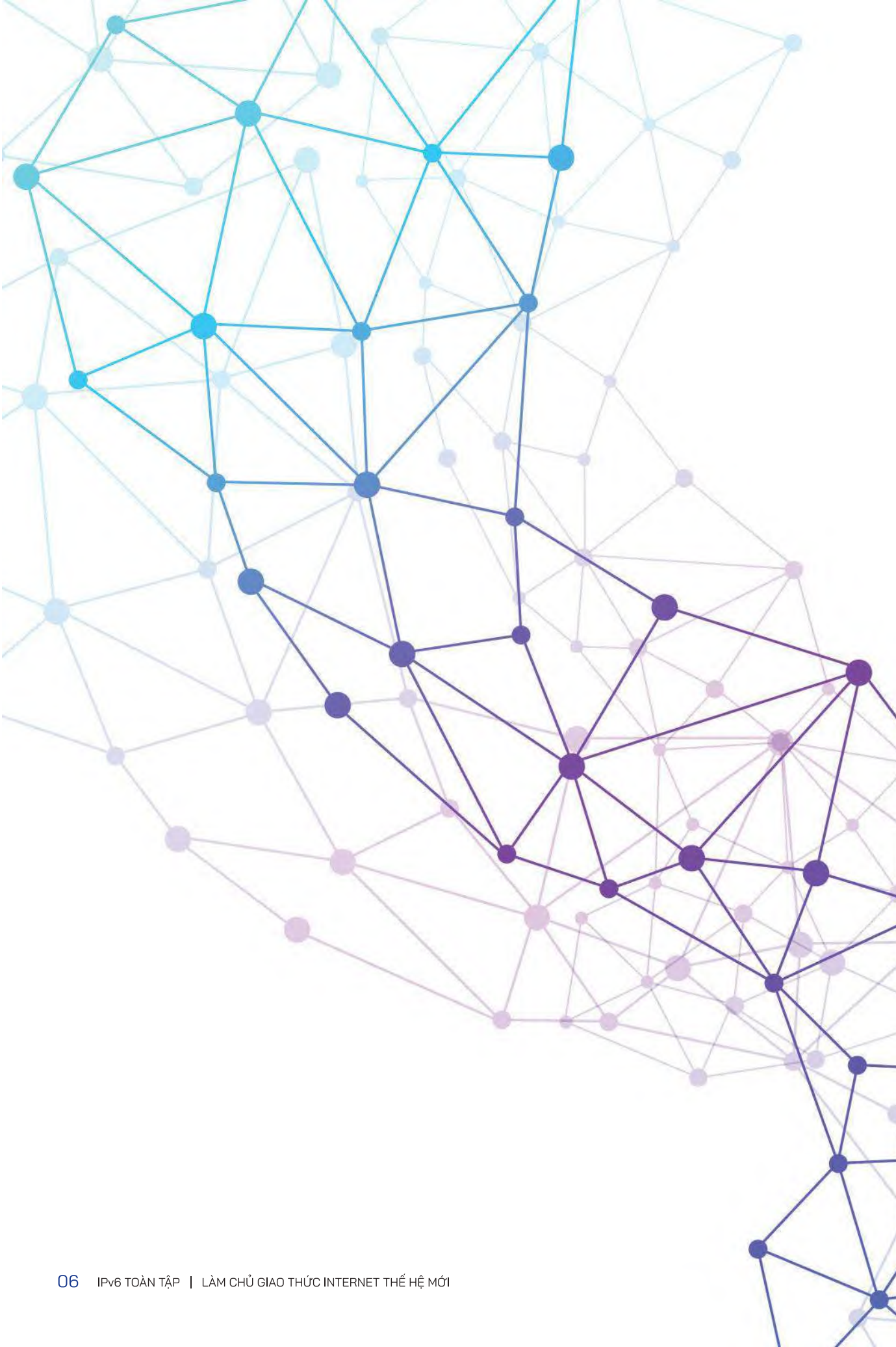
Tuy nhiên, để tiến xa hơn, Việt Nam cần một tài liệu chuyên sâu, bài bản và thực tiễn để hỗ trợ triển khai IPv6 trong thực tế. Các tổ chức, doanh nghiệp, chuyên gia kỹ thuật, các trường đại học cần một cuốn cẩm nang vừa cung cấp kiến thức, vừa hướng dẫn chi tiết quy hoạch địa chỉ, thiết lập hệ thống và chuyển đổi từ IPv4 sang Dual Stack và từ Dual Stack sang IPv6 Only.

"IPv6 toàn tập – Làm chủ giao thức Internet thế hệ mới" ra đời nhằm đáp ứng nhu cầu đó và là tài liệu hữu ích cho các sinh viên, kỹ sư, quản trị hệ thống và những người đang chuẩn bị cho tương lai số. Cuốn sách không chỉ đi từ căn bản đến nâng cao, mà còn tích hợp ví dụ thực tế, bài tập và công cụ hỗ trợ, giúp triển khai IPv6 hiệu quả, tiết kiệm và an toàn.

Đây cũng là lời tri ân đến cộng đồng công nghệ Việt Nam - những người đang kiến tạo tương lai số cho đất nước. Hành trình từ IPv4 sang IPv6 không chỉ là đổi mới kỹ thuật, mà là cuộc cách mạng xây dựng nền tảng Internet sẵn sàng cho IoT, 5G, AI và các công nghệ tương lai.

Hãy cùng VNNIC khám phá, học hỏi và làm chủ IPv6 – vì một Việt Nam số an toàn, hiện đại và hội nhập.

Trung tâm Internet Việt Nam (VNNIC)



MỤC LỤC

DANH MỤC HÌNH VẼ **11**

DANH MỤC BẢNG BIỂU **15**

DANH MỤC TỪ VIẾT TẮT **15**

PHẦN 1 – LÝ THUYẾT **19**

CHƯƠNG 1: TỔNG QUAN VỀ GIAO THỨC IPv4 & IPv6 ..... **20**

1.1 Vài nét lịch sử về IPv4 21

1.2 Lịch sử phát triển của mạng Internet 21

1.3 Các giải pháp tình thế cho vấn đề của IPv4 22

1.4 Câu chuyện ra đời của IPv6 24

1.5 Các phiên bản IP khác ở đâu? 26

1.6 Địa chỉ IPv6 nhiều như thế nào? 27

1.7 Hiện trạng chuyển đổi sang IPv6 trên thế giới 28

1.8 Những cột mốc triển khai IPv6 tại Việt Nam và mục tiêu IPv6 Only 29

1.9 Vai trò của IPv6 với mạng 5G 31

1.10 Vai trò của IPv6 với IoT 34

1.11 Những lợi ích IPv6 mang lại 36

1.12 Phân vùng không gian địa chỉ IPv6 37

1.13 Cơ quan quản lý và cấp phát địa chỉ IP 38

1.14 Giới thiệu về Trung tâm Internet Việt Nam (VNNIC) 40

1.15 Tổng kết chương 1 40

1.16 Câu hỏi ôn tập chương 1 41

CHƯƠNG 2: CẤU TRÚC VÀ ĐẶC ĐIỂM GIAO THỨC IPv6 ..... **42**

2.1 IPv4, IPv6 và bộ giao thức TCP/IP 44

2.2 Cấu trúc bản tin của IPv6 và những cải tiến 45

2.3 Tiêu đề mở rộng (Extension Header) 47

2.4 Tổng kết chương 2 50

2.5 Câu hỏi ôn tập chương 2 50

CHƯƠNG 3: CHI TIẾT CÁC LOẠI ĐỊA CHỈ IPv6 ..... **51**

3.1 Cách biểu diễn địa chỉ IPv6 53

3.2 Phân loại địa chỉ IPv6 54

3.3 Vị trí phân vùng các loại địa chỉ IPv6 56

3.4 Địa chỉ Global Unicast Address (GUA) 58

3.5 Địa chỉ Unique Local Address (ULA) 59

3.6 Địa chỉ Link Local Address (LLA) 61

3.7 Địa chỉ Unspecified 62

3.8 Địa chỉ Loopback 62

3.9 Địa chỉ IPv4 Embeded 63
3.10 Địa chỉ Multicast 64
3.11 Địa chỉ Well-known Multicast 67
3.12 Địa chỉ Solicited-Node Multicast 68
3.13 Quy tắc lựa chọn địa chỉ IPv6 69
3.14 Quy tắc 6: Policy Table 71
3.15 Tổng kết chương 3 72
3.16 Câu hỏi ôn tập chương 3 72
CHƯƠNG 4: GIAO THỨC ICMPv6, NDP & CÁC KỸ THUẬT, DỊCH VỤ MẠNG PHỔ BIẾN 74
4.1 Tổng quan về giao thức ICMP 76
4.2 Phân loại bản tin ICMP 77
4.3 Các nhóm bản tin ICMP Querry Message 78
4.4 Các nhóm bản tin ICMP Error Message 79
4.5 Một số công cụ, kỹ thuật sử dụng ICMP 80
4.5.1 Lệnh PING 80
4.5.2 Lệnh TRACERT/TRACEROUTE 81
4.5.3 Kỹ thuật Path MTU Discovery (PMTUD) 82
4.6 Giao thức ICMPv6 83
4.7 Giao thức NDP 85
4.8 Kỹ thuật gán địa chỉ tự động SLAAC 86
4.9 Stateless DHCPv6 88
4.10 Stateful DHCPv6 89
4.11 EUI-64 tạo Interface-ID theo địa chỉ MAC 91
4.12 RFC 4941 tạo Interface-ID ngẫu nhiên 92
4.13 Các trạng thái hoạt động của địa chỉ IPv6 93
4.14 Kỹ thuật phân giải địa chỉ MAC 94
4.15 Các trạng thái trong Neighbor Cache 95
4.16 Kỹ thuật kiểm trùng địa chỉ DAD 96
4.17 Kỹ thuật dò tìm IPv6 Path MTU (PMTU) 97
4.18 Tổng kết chương 4 98
4.19 Câu hỏi ôn tập chương 4 98
CHƯƠNG 5: CÁC KỸ THUẬT CHUYỂN ĐỔI TỪ IPv4 SANG IPv6 101
5.1 Những thách thức và yêu cầu 103
5.2 Kỹ thuật Dual Stack 103
5.3 Kỹ thuật Tunneling 104
5.4 Kỹ thuật Translation 105
5.5 Chuyển đổi IPv6 cho mạng MPLS 106
5.5.1 6PE (IPv6 Provider Edge) 106
5.5.2 6VPE (IPv6 VPN Provider Edge) 107
5.6 Xây dựng kế hoạch chuyển đổi IPv6 108
5.6.1 Giai đoạn 1: Chuẩn bị 108
5.6.2 Giai đoạn 2: Kết nối và thử nghiệm 109
5.6.3 Giai đoạn 3: Chuyển đổi chính thức 109
5.7 Tổng kết chương 5 109
5.8 Câu hỏi ôn tập chương 5 110

CHƯƠNG 6: CÁC KỸ THUẬT TRIỂN KHAI IPv6 ONLY **111**

6.1 Giới thiệu về IPv6 Only và các giai đoạn chuyển đổi 113
6.2 Lợi ích khi chuyển đổi sang IPv6 Only 113
6.3 Các chính sách, công nghệ về IPv6 Only 114
6.4 IPv6+ tương lai của IPv6 Only 114
6.4.1 Đặc điểm nổi bật của IPv6+ 115
6.4.2 Ứng dụng thực tế 116
6.5 Giải pháp kỹ thuật cho IPv6 Only 116
6.6 Kỹ thuật DNS64/NAT64 118
6.7 Kỹ thuật Dual Stack Lite (DS Lite) 119
6.8 Kỹ thuật 464XLAT 120
6.9 Tổng kết chương 6 121
6.10 Câu hỏi ôn tập chương 6 122

CHƯƠNG 7: HƯỚNG DẪN QUY HOẠCH ĐỊA CHỈ IPv6 ..... **124**

7.1 Yêu cầu và nguyên tắc chung đối với việc quy hoạch IPv6 126
7.1.1 Yêu cầu của việc quy hoạch 126
7.1.2 Khác biệt giữa quy hoạch địa chỉ IPv4 và IPv6 126
7.1.3 Những nguyên tắc khi quy hoạch địa chỉ IPv6 127
7.2 Những chú ý trước khi quy hoạch địa chỉ IPv6 127
7.2.1 Subnet bit để quy hoạch IPv6 128
7.2.2 Quy hoạch theo phạm vi 4 bit (Nibble Boundary) 128
7.2.3 Một số quy định về IPv6 Prefix Length 130
7.3 Cách thức quy hoạch địa chỉ IPv6 131
7.3.1 Phân tầng hóa hệ thống mạng 131
7.3.2 Phân chia Subnet theo số bit 132
7.4 Minh họa quy hoạch IPv6 cho một doanh nghiệp 133
7.5 Hướng dẫn sử dụng công cụ phân chia Subnet IPv6 134
7.6 Kết hợp công cụ chia Subnet và File Excel 135
7.7 Tổng kết chương 7 137
7.8 Câu hỏi ôn tập chương 7 138

PHẦN 2 – THỰC HÀNH **141**

CHƯƠNG 8: HƯỚNG DẪN TRIỂN KHAI MÔ HÌNH IPv6 DUAL STACK **141**

8.1 Mô hình mạng hiện đại Dual Stack cho doanh nghiệp, cơ quan và tổ chức với IP/ASN độc lập và đa hướng 142
8.2 Mô hình và nội dung LAB IPv6 Dual Stack 143
8.3 Các bài LAB chi tiết cho mô hình Dual Stack 144
8.4 LAB01 - Cấu hình địa chỉ IPv6 tĩnh cho router 145
8.5 LAB02 - Cấu hình địa chỉ IPv6 tĩnh cho Windows và Ubuntu 146
8.5.1 Khai báo IPv6 cho Windows 146
8.5.2 Khai báo IPv6 cho Ubuntu 147
8.6 LAB03 -Cấu hình địa chỉ IPv6 động bằng SLAAC 150
8.7 LAB04 - Cấu hình địa chỉ IPv6 động bằng Stateful DHCPv6 151
8.8 LAB05 - Cấu hình địa chỉ IPv6 động bằng Stateless DHCPv6 152

8.9 LAB06 - Cấu hình giao thức dự phòng VRRPv3 153
8.10 LAB07 - Cấu hình định tuyến tĩnh (Static Route) 155
8.11 LAB08 - Cấu hình giao thức định tuyến OSPFv3 156
8.12 LAB09 - Cấu hình giao thức định tuyến iBGP 159
8.13 LAB10 - Cấu hình giao thức định tuyến eBGP 161
8.14 Tổng kết chương 8 163
8.15 Câu hỏi ôn tập chương 8 164

CHƯƠNG 9: HƯỚNG DẪN TRIỂN KHAI MÔ HÌNH IPv6-ONLY 167

9.1 Mô hình mạng tiên tiến IPv6 Only cho doanh nghiệp, cơ quan và tổ chức với DNS64 và NAT64 168
9.2 Mô hình và nội dung LAB IPv6 Only 169
9.3 Các bài LAB chi tiết cho mô hình IPv6 Only 170
9.4 LAB01- Sử dụng Dynamic NAT64 cho Outbound NAT 171
9.5 LAB02 – Sử dụng Overload NAT64 cho Outbound NAT 174
9.6 LAB03 - Sử dụng Static NAT64 cho Inbound NAT 174
9.7 LAB04 - Sử dụng DNS64 Server chế độ IPv6 Only làm Resolver cho kết nối Outbound 176
9.8 LAB05 - Kiểm tra hoạt động của DNS64 và NAT64 cho kết nối Outbound 179
9.9 LAB06 - Sử dụng DNS64 chế độ Dual Stack làm Authoritative Server cho kết nối Inbound 181
9.10 LAB07 - Mô hình tích hợp DNS64/NAT64 186
9.11 Tổng kết chương 9 190
9.12 Câu hỏi ôn tập chương 9 190

CHƯƠNG 10: HƯỚNG DẪN KIỂM TRA VÀ ĐÁNH GIÁ KẾT QUẢ TRIỂN KHAI IPv6 VÀ IPv6 ONLY 193

10.1 Các nội dung cần kiểm tra, đánh giá 194
10.2 Tổng quan về ứng dụng i-SPEED by VNNIC 194
10.3 Kiểm tra, đánh giá hạ tầng mạng đã sẵn sàng với IPv6 195
10.3.1 Sử dụng trang: speedtest.vn 195
10.3.2 Sử dụng ứng dụng i-Speed by VNNIC 196
10.3.3 Sử dụng trang: test-ipv6.com 197
10.3.4 Sử dụng trang: ipv6-test.com 198
10.4 Kiểm tra dịch vụ cung cấp ra bên ngoài hoạt động với IPv6 198
10.4.1 Kiểm tra bằng trang ipv6-test.com 198
10.4.2 Kiểm tra bằng trang: ready.chair6.net 199
10.4.3 Kiểm tra bằng máy tính IPv6 Only 200
10.5 Hướng dẫn gắn Logo "IPv6 Ready" cho Website 202
10.6 Tổng kết chương 10 203
10.7 Câu hỏi ôn tập chương 10 203

PHỤ LỤC 205

Các RFC phổ biến về IPv6 205

Tài liệu tham khảo 206

DANH MỤC HÌNH VẼ

Hình 1. Mạng NSFNet giai đoạn 1991 21
Hình 2. Số lượng người dùng Internet qua các năm 22
Hình 3. Quá trình cạn kiệt địa chỉ IPv4 của các tổ chức quản lý tài nguyên cấp vùng 23
Hình 4. Chi tiết ISO Protocol Stack 24
Hình 5. Lịch sử ra đời của IPv6 và các giao thức, hoạt động hỗ trợ 25
Hình 6. Cấu trúc địa chỉ IPv6 Global Unicast 27
Hình 7. Minh họa số lượng địa chỉ IPv6 27
Hình 8. Tỉ lệ người dùng IPv6 qua các năm 28
Hình 9. Công bố của VNNIC về tỷ lệ người dùng IPv6 tại Việt Nam 30
Hình 10. Lộ trình dự kiến tắt IPv4 chuyển sang IPv6 Only từ VNNIC 31
Hình 11. Các đặc trưng của mạng 5G 31
Hình 12. Số liệu mạng 5G và 5G SA 33
Hình 13. Thị trường 5G Stand Alone dự kiến 33
Hình 14. Các công nghệ trong IoT 34
Hình 15. Các chuẩn giao thức IoT liên quan đến IPv6 35
Hình 16. Các vùng địa chỉ IPv6 37
Hình 17. Số lượng dãy địa chỉ IPv6 phân bổ cho RIR 37
Hình 18. Tên 5 tổ chức quản lý vùng và thời gian thành lập 38
Hình 19. Phạm vi quản lý của 5 tổ chức cấp vùng 38
Hình 20. Mối liên hệ giữa IANA, các RIR & NIR 39
Hình 21. Số liệu về địa chỉ IP/ASN do VNNIC cấp 40
Hình 22. IPv4, IPv6 và các giao thức hỗ trợ 44
Hình 23. So sánh IPv4 và IPv6 Header 45
Hình 24. Những trường của IPv4 được giữ lại và bị xóa bỏ khỏi IPv6 46
Hình 25. Chi tiết các trường của IPv6 47
Hình 26. Ý nghĩa của trường Next Header 47
Hình 27. Vị trí của Extension Header 48
Hình 28. Vị trí AH và các Extension Header khác ở chế độ Transport và Tunnel 49
Hình 29. Vị trí ESP và các Extension Header khác ở chế độ Transport và Tunnel 49
Hình 30. Minh họa cách viết rút gọn địa chỉ IPv6 54
Hình 31. Cách thức hoạt động của các loại địa chỉ 54
Hình 32. Phân loại địa chỉ IPv6 theo cách thức hoạt động 55
Hình 33. Phân loại địa chỉ IPv6 theo phạm vi hoạt động 56
Hình 34. Chi tiết phân loại IPv6 theo cách thức và phạm vi hoạt động 56
Hình 35. Chi tiết các loại địa chỉ IPv6 theo các phân vùng 57
Hình 36. Cấu trúc của địa chỉ GUA được phân bổ thực tế 58
Hình 37. Cấu trúc của địa chỉ ULA 59
Hình 38. Mô hình hoạt động với NPTv6 60
Hình 39. Cấu trúc của địa chỉ LLA 61
Hình 40. Địa chỉ Unicast đặc biệt Unspecified 62
Hình 41. Địa chỉ Unicast đặc biệt Loopback 62
Hình 42. Địa chỉ Unicast đặc biệt IP4-Embeded 63
Hình 43. Địa chỉ Unicast đặc biệt IPv4-compatible không còn được sử dụng 63

Hình 44. Cấu trúc địa chỉ IPv6 đặc biệt IP4-Mapped 63
Hình 45. Thành phần của địa chỉ IPv6 Muticast 64
Hình 46. Cấu trúc của địa chỉ Multicast 64
Hình 47. Minh họa Scope của địa chỉ Multicast 65
Hình 48. Ethernet Frame của bản tin IPv6 Multicast 66
Hình 49. Ethernet Frame của bản tin IPv4 Multicast 66
Hình 50. Nguyên tắc tạo Solicited-Node Multicast từ Unicast 68
Hình 51. Ví dụ nguyên tắc tạo Solicited-Node Multicast từ Unicast 68
Hình 52. Minh họa truy cập Internet ở chế độ Dual Stack 69
Hình 53. Nguyên tắc Longest prefix matching giữa địa chỉ nguồn và đích 70
Hình 54. Chi tiết Policy Table 71
Hình 55. Giao thức IP và các giao thức hỗ trợ 76
Hình 56. Cấu trúc bản tin ICMP 76
Hình 57. Chi tiết nhóm bản tin ICMP Querry 78
Hình 58. Chi tiết nhóm bản tin ICMP Querry 79
Hình 59. Hoạt động của bản tin ICMP Redirect 80
Hình 60. Các bản tin trong lệnh Ping 80
Hình 61. Thông tin trả về của lệnh Ping 81
Hình 62. Chi tiết hoạt động của lệnh Trace 81
Hình 63. Thông tin trả về của lệnh Trace 81
Hình 64. Chi tiết hoạt động của PMTU 82
Hình 65. Định dạng chung của bản tin ICMPv6 83
Hình 66. Hai nhóm bản tin chính của ICMPv6 và của NDP, MLD 83
Hình 67. Chi tiết các bản tin của ICMPv6 và NDP, MLD 84
Hình 68. Chi tiết của các bản tin của NDP 85
Hình 69. Cấu trúc 2 bản tin Router Solicitation và Router Advertisement 85
Hình 70. Hoạt động của Router Solicitation và Router Advertisement 85
Hình 71. Hoạt động của Neighbor Solicitation và Neighbor Advertisement 86
Hình 72. Chi tiết hoạt động của SLAAC 86
Hình 73. Thông tin về giao thức NDP và SLAAC trên cổng Router 87
Hình 74. Cấu trúc bản tin Router Advertisement 88
Hình 75. Trạng thái của Interface khi khai báo Stateless DHCP 89
Hình 76. Chi tiết hoạt động của Statefull DHCPv6 90
Hình 77. Chi tiết nguyên tắc của EUI-64 91
Hình 78. Địa chỉ IPv6 chính và tạm thời 92
Hình 79. Các trạng thái của địa chỉ IPv6 93
Hình 80. Các bản tin trong kỹ thuật phân giải địa chỉ MAC và IPv6 94
Hình 81. Chi tiết các trạng thái của Neighbor Cache 95
Hình 82. Các bản tin trong kỹ thuật phân kiểm trùng địa chỉ 96
Hình 83. Hoạt động của IPv6 Path MTU 97
Hình 84. Hoạt động của cơ chế Dual Stack 104
Hình 85. Hoạt động của cơ chế Tunnel 104
Hình 86. Kỹ thuật NAT cho mạng IPv6 Only 105
Hình 87. Hoạt động của cơ chế 6PE 107
Hình 88. Hoạt động của cơ chế 6VPE 107

Hình 89. Lộ trình chuyển đổi IPv6 do VNNIC đề xuất 108
Hình 90. Các giai đoạn chuyển đổi từ IPv4 sang IPv6 113
Hình 91. Đặc điểm và lợi ích của IPv6+ (nguồn: Roland Berger) 115
Hình 92. IPv6+ hỗ trợ tốt cho 5G/Cloud/IoT 116
Hình 93. Các công nghệ cho IPv6 Only đối với Internet băng rộng cố định 117
Hình 94. Các công nghệ cho IPv6 Only đối với Internet băng rộng di động 117
Hình 95. Nguyên tắc hoạt động của DNS64 và NAT64 118
Hình 96. Nguyên tắc hoạt động của giải pháp DS-Lite 119
Hình 97. Nguyên tắc hoạt động của giải pháp DS-Lite 121
Hình 98. Vị trí Subnet bit trong địa chỉ IPv6 GUA 128
Hình 99. Cách thức phân chia theo Nibble 129
Hình 100. Ví dụ về phân chia Subnet theo Nibble 129
Hình 101. Ví dụ về phân chia Subnet không theo Nibble 129
Hình 102. Một số Prefix Length đặc biệt 130
Hình 103. Minh họa việc phân tầng hóa hệ thống 131
Hình 104. Ví dụ việc phân tầng IPv6 cho doanh nghiệp 131
Hình 105. Ví dụ việc phân tầng cho nhà mạng 132
Hình 106. Nguyên tắc phân chia theo số bit từ trái sang phải 132
Hình 107. Minh họa việc phân tầng và phân bổ Prefix Length cho một doanh nghiệp 133
Hình 108. Giao diện của công cụ phân chia địa chỉ IPv6 trực tuyến 135
Hình 109. Thực hiện phân chia Network ban đầu thành Subnet nhỏ hơn 135
Hình 110. Thực hiện tương tự cho các Subnet ở Level thấp hơn 136
Hình 111. Mô hình mạng hiện đại với IP/ASN độc lập và kết nối đa hướng 142
Hình 112. Mô hình LAB tổng thể 143
Hình 113. Chi tiết thông tin quy hoạch cho bài LAB 144
Hình 114. Chi tiết quy hoạch và phân bổ địa chỉ IPv6 cho các Level 145
Hình 115. Hướng dẫn khai báo IPv6 cho Windows 147
Hình 116. Kiểm tra tên Card mạng 147
Hình 117. Kiểm tra tên của File cấu hình của Netplan 148
Hình 118. Lệnh để sửa File cấu hình Netplan 148
Hình 119. Thay đổi thông tin tương ứng với quy hoạch của bài LAB 148
Hình 120. Áp dụng khai báo mới cho Netplan 148
Hình 121. Kiểm tra kết quả sau khai báo 148
Hình 122. Kiểm tra IPv6 Gateway 149
Hình 123. Kiểm tra đầy đủ các thông tin về địa chỉ IPv4, IPv6 149
Hình 124. Mô hình của bài LAB về SLAAC 150
Hình 125. Kiểm tra địa chỉ IPv6 Client nhận được 152
Hình 126. Mô hình của bài LAB về VRRPv3 153
Hình 127. SLAAC vẫn hoạt động tốt với VRRPv3 155
Hình 128. Mô hình của bài LAB về Static Route 155
Hình 129. Mô hình của bài LAB về OSPFv3 156
Hình 130. Mô hình của bài LAB về iBGP 159
Hình 131. Mô hình của bài LAB về eBGP 161
Hình 132. Mô hình mạng hiện đại với IP/ASN độc lập và kết nối đa hướng 168
Hình 133. Mô hình LAB IPv6 Only với NAT64 và DNS64 độc lập 169

Hình 134. Mô hình LAB IPv6 Only với NAT64 và DNS64 được tích hợp 169
Hình 135. Mô hình LAB trên phần mềm EVE-NG 170
Hình 136. Mô hình của bài LAB về Dynamic NAT64 171
Hình 137. Mô hình kiểm tra của bài LAB về Dynamic NAT64 172
Hình 138. Mô hình của bài LAB về Static NAT64 174
Hình 139. Mô hình của bài LAB sử dụng IPv6 Only DNS64 176
Hình 140. Khai báo cho named.conf.options 177
Hình 141. Khai báo cho named.conf.local 177
Hình 142. Khai báo cho db.ipv4only.com 178
Hình 143. Kiểm tra khai báo cho Netplan 179
Hình 144. Khai báo nameserver cho /etc/resolv.conf 179
Hình 145. Thực hiện lệnh PING đến máy tính IPv4 Only 180
Hình 146. Mô hình của bài LAB sử dụng Dual Stack DNS64 181
Hình 147. Khai báo cho Netplan 182
Hình 148. Khai báo cho named.conf.local 182
Hình 149. Khai báo cho Zone ipv4only.com 183
Hình 150. Khai báo cho Zone ipv6only.com 183
Hình 151. Khai báo cho Zone ngược ipv4only.com 184
Hình 152. Khai báo cho Zone ngược ipv6only.com 184
Hình 153. Thực hiện PING kiểm tra máy tính IPv4 Only từ máy tính IPv6 Only 185
Hình 154. Thực hiện PING kiểm tra máy tính IPv6 Only từ máy tính IPv4 Only 185
Hình 155. Kiểm tra phân giải ngược cho địa chỉ IPv6 185
Hình 156. Kiểm tra phân giải ngược cho địa chỉ IPv4 186
Hình 157. Mô hình của bài LAB IPv6 Only tích hợp giữa NAT64 và DNS64 186
Hình 158. Các khai báo cho DNS64 187
Hình 159. Kiểm tra kác khai báo cho DNS64 188
Hình 160. Cập nhật các gói phần mềm trước khi cài đặt Jool 188
Hình 161. Tải và cài đặt phần mềm Jool 188
Hình 162. Kiểm tra hoạt động của Jool sau khai báo 189
Hình 163. Kiểm tra hoạt động của Jool và Bind sau khi cấu hình 189
Hình 164. Giới thiệu về i-Speed by VNNIC 194
Hình 165. Kiếm tra trên máy tính, trường hợp mạng hỗ trợ IPv6 195
Hình 166. Kiếm tra trên điện thoại, trường hợp mạng không hỗ trợ IPv6 196
Hình 167. Cách kiểm tra hỗ trợ IPv6 bằng ứng dụng i-Speeed 197
Hình 168. Cách kiểm tra hỗ trợ IPv6 tại test-ipv6.com 197
Hình 169. Cách kiểm tra hỗ trợ IPv6 tại ipv6-test.com 198
Hình 170. Kiểm tra máy chủ Web hỗ trợ IPv6 tại ipv6-test.com 199
Hình 171. Giao diện của trang ready.chair6.net 199
Hình 172. Kết quả kiểm tra từ trang ready.chair6.net 200
Hình 173. Khai báo IPv6 Only cho máy tính thực hiện kiểm tra 201
Hình 174. Kiểm tra máy chủ dịch vụ từ máy tính IPv6 Only 201
Hình 175. Kiểm tra máy chủ dịch vụ khanhhoa.gov.vn 202
Hình 176. Logo IPv6 Ready do ipv6-test.com cung cấp 202

DANH MỤC BẢNG BIỂU

Bảng 1. Tóm tắt các phiên bản của giao thức Internet Protocol 26
Bảng 2. Một số Extension Header phổ biến 48
Bảng 3. Đặc điểm của địa chỉ IPv6 53
Bảng 4. Danh sách Scope của IPv6 Multicast 65
Bảng 5. Danh sách địa chỉ Well-known Multicast 67
Bảng 6. Chi tiết các bản tin ICMP 77
Bảng 7. So sánh các bản tin giữa ICMPv4 và ICMPv6 84
Bảng 8. Tóm tắt một số kỹ thuật Tunnel 105
Bảng 9. So sánh một số đặc điểm của IPv4 và IPv6 129
Bảng 10. Lưu trữ thông tin quy hoạch bằng Excel 133
Bảng 11. Điền thông tin vào Excel 136
Bảng 12. Chi tiết quy hoạch và phân bổ địa chỉ IPv6 cho các Level trung gian 136
Bảng 13. Chi tiết quy hoạch và phân bổ địa chỉ IPv6 cho các Level cuối cùng 137
Bảng 14. Các bài LAB chi tiết cho mạng Dual Stack 144
Bảng 15. Các bài LAB chi tiết kết hợp giữa NAT64 và DNS64 170
Bảng 16. Danh sách những RFC phổ biến nhất liên quan đến IPv6 206

DANH MỤC TỪ VIẾT TẮT

THUẬT NGỮ/ TỪ VIẾT TẮT	TÊN ĐẦY ĐỦ	MÔ TẢ
464XLAT	464XLAT	Giải pháp chuyển đổi hỗ trợ ứng dụng IPv4 chạy trên môi trường IPv6 Only.
5G NSA	5G Non-Standalone	Kiến trúc mạng 5G sử dụng hạ tầng LTE hiện có.
5G SA	5G Standalone	Kiến trúc mạng 5G độc lập, không phụ thuộc vào LTE.
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks	Chuẩn cho việc truyền tải gói tin IPv6 qua các mạng không dây công suất thấp (IoT).
6PE	IPv6 Provider Edge	Kỹ thuật triển khai IPv6 cho Router biên của nhà cung cấp dịch vụ trong môi trường MPLS.
6RD	IPv6 Rapid Deployment	Phương pháp triển khai nhanh IPv6 qua hạ tầng IPv4 hiện có.
6to4	6to4 Tunnel	Cơ chế tự động tạo đường hầm cho IPv6 qua mạng IPv4.
6VPE	IPv6 VPN Provider Edge	Giải pháp triển khai IPv6 cho các dịch vụ VPN trên hạ tầng MPLS của nhà cung cấp.
AAAA Record	Quad-A (AAAA) Record	Bản ghi DNS ánh xạ tên miền thành địa chỉ IPv6.
AfriNIC	African Network Information Centre	Tổ chức quản lý tài nguyên Internet cho khu vực châu Phi.
AH	Authentication Header	Thành phần của IPSec đảm bảo xác thực gói tin.

THUẬT NGỮ/ TỪ VIẾT TẮT	TÊN ĐẦY ĐỦ	MÔ TẢ
APNIC	Asia-Pacific Network Information Centre	Tổ chức quản lý tài nguyên Internet IP/ASN khu vực Châu Á - Thái Bình Dương
ARP	Address Resolution Protocol	Giao thức phân giải địa chỉ IP sang địa chỉ vật lý (cho IPv4).
BGP	Border Gateway Protocol	Giao thức định tuyến giữa các hệ thống mạng tự quản trên Internet.
BIND	Berkeley Internet Name Domain	Phần mềm máy chủ DNS phổ biến.
CIDR	Classless Inter-Domain Routing	Phương pháp phân bổ địa chỉ IP không theo lớp truyền thống.
CLAT	Customer-side Translator	Thành phần chuyển đổi ở phía khách hàng trong giải pháp 464XLAT.
DHCP	Dynamic Host Configuration Protocol	Giao thức cấp phát địa chỉ IP tự động cho thiết bị.
DNS	Domain Name System	Hệ thống phân giải tên miền sang địa chỉ IP.
DNS64	DNS64	Cơ chế ánh xạ tên miền IPv4 thành bản ghi IPv6 để hỗ trợ NAT64.
DS-Lite	Dual Stack Lite	Giải pháp kết nối IPv4 qua mạng IPv6 mà không cần địa chỉ IPv4 công khai.
ESP	Encapsulating Security Payload	Thành phần của IPSec cung cấp bảo mật dữ liệu qua mã hóa.
EUI-64	Extended Unique Identifier 64bit	Phương pháp tạo Interface ID cho IPv6 dựa trên địa chỉ MAC.
GUA	Global Unicast Address	Địa chỉ IPv6 định tuyến toàn cầu.
Hextex	Hexadecimal Text Representation	Biểu diễn địa chỉ IPv6 dưới dạng số hệ thập lục phân.
IAB	Internet Architecture Board	Cơ quan tư vấn về kiến trúc và phát triển Internet.
IANA	Internet Assigned Numbers Authority	Là cơ quan trực thuộc ICANN, chịu trách nhiệm quản lý máy chủ DNS Root, địa chỉ IP, số hiệu mạng ASN và tham số của các giao thức mạng.
ICANN	Internet Corporation for Assigned Names and Numbers	Tổ chức quản lý tên, số toàn cầu
ICMPv6	Internet Control Message Protocol for IPv6	Giao thức báo lỗi và chẩn đoán hoạt động của mạng IPv6.
IETF	Internet Engineering Task Force	Tổ chức chuẩn hóa các giao thức và công nghệ Internet.
IGMP	Internet Group Management Protocol	Giao thức quản lý thành viên của nhóm Multicast (IPv4).

THUẬT NGỮ/ TỪ VIẾT TẮT	TÊN ĐẦY ĐỦ	MÔ TẢ
IPSec	Internet Protocol Security	Bộ giao thức bảo mật cho giao tiếp qua IP.
Jool	Jool	Ứng dụng mã nguồn mở cho NAT64 và SIIT.
LLA	Link-Local Address	Địa chỉ IPv6 chỉ hoạt động trong phạm vi một liên kết mạng cụ thể.
LPWAN	Low-Power Wide-Area Network	Mạng diện rộng có công suất thấp, thường áp dụng cho thiết bị IoT.
MLD	Multicast Listener Discovery	Giao thức quản lý thành viên của nhóm multicast trong IPv6.
MPLS	Multiprotocol Label Switching	Công nghệ chuyển mạch nhãn đa giao thức, hỗ trợ định tuyến nhanh.
MTU	Maximum Transmission Unit	Kích thước tối đa của gói tin có thể truyền qua một liên kết mạng.
NA	Neighbor Advertisement	Thông điệp phản hồi thông tin từ node lân cận trong IPv6.
NAT	Network Address Translation	Kỹ thuật chuyển đổi giữa các địa chỉ IP
NAT64	Network Address Translation 64	Kỹ thuật chuyển đổi địa chỉ giữa IPv6 và IPv4.
NDP	Neighbor Discovery Protocol	Giao thức thay thế ARP trong IPv6, quản lý thông tin của các node lân cận.
Nibble	Nibble	Đơn vị thông tin gồm 4 bit, dùng trong biểu diễn địa chỉ IPv6.
NIR	National Internet Registry	Tổ chức quản lý địa chỉ Internet, số hiệu mạng (ASN) cấp quốc gia
NPTv6	Network Prefix Translation for IPv6	Cơ chế chuyển đổi tiền tố mạng trong IPv6.
NS	Neighbor Solicitation	Thông điệp yêu cầu phản hồi từ node lân cận trong IPv6.
PLAT	Provider-side Translator	Thành phần chuyển đổi ở phía nhà cung cấp trong giải pháp 464XLAT.
PMTUD	Path MTU Discovery	Cơ chế tìm kiếm kích thước MTU tối ưu trên đường truyền.
PTB	Packet Too Big	Thông điệp lỗi ICMPv6 báo hiệu gói tin vượt quá kích thước MTU của liên kết.
RA	Router Advertisement	Thông điệp quảng bá thông tin cấu hình từ Router trong IPv6.
RIPE NCC	Réseaux IP Européens Network Coordination Centre	Tổ chức quản lý tài nguyên Internet IP/ASN khu vực Châu Âu và Trung Đông

THUẬT NGỮ/ TỪ VIẾT TẮT	TÊN ĐẦY ĐỦ	MÔ TẢ
RIR	Regional Internet Registry	Các tổ chức quản lý địa chỉ IP theo khu vực địa lý.
RS	Router Solicitation	Thông điệp yêu cầu thông tin cấu hình từ Router trong IPv6.
SIPP	Simple Internet Protocol Plus	Đề xuất cải tiến giao thức IP trong quá trình chuyển đổi sang IPv6.
SLAAC	Stateless Address Autoconfiguration	Cơ chế tự động cấu hình địa chỉ IPv6 mà không cần DHCP.
SRv6	Segment Routing over IPv6	Kỹ thuật định tuyến dựa trên phân đoạn trong IPv6.
TCP/IP	Transmission Control Protocol/Internet Protocol	Bộ giao thức truyền thông cơ bản cho mạng máy tính và Internet.
TUBA	TCP/UDP with Bigger Addresses	Đề xuất mở rộng giao thức TCP/UDP nhằm hỗ trợ không gian địa chỉ IP lớn.
ULA	Unique Local Address	Địa chỉ IPv6 dùng cho mạng nội bộ, không định tuyến trên Internet.
VLSM	Variable Length Subnet Mask	Kỹ thuật phân chia mạng con với độ dài Subnet Mask khác nhau.
VNNIC	Vietnam Internet Network Information Center	Trung tâm Internet Việt Nam, quản lý, phân bổ, cấp tài nguyên Internet Việt Nam (tên miền .vn, địa chỉ IP, ASN)

PHẦN 1 – LÝ THUYẾT

CHƯƠNG 1

TỔNG QUAN VỀ GIAO THỨC IPv4 & IPv6

CHƯƠNG 1

TỔNG QUAN VỀ GIAO THỨC IPv4 & IPv6

Khi mạng máy tính ra đời, nhiều giao thức đã được phát triển, nhưng TCP/IP phiên bản 4 (IPv4) với những ưu điểm vượt trội đã trở thành nền tảng duy nhất của Internet. Tuy nhiên, sự phát triển nhanh chóng của Internet đã bộc lộ các hạn chế của IPv4, đặc biệt là không gian địa chỉ hạn chế, từ đó thúc đẩy sự ra đời của giao thức IPv6.

Hành trình từ IPv4 đến IPv6 là một quá trình dài và không đơn giản, nhưng đến nay, IPv6 đã được đón nhận rộng rãi bởi các cơ quan, doanh nghiệp và người dùng toàn cầu.

Chương 1 sẽ giới thiệu lịch sử phát triển của giao thức Internet, làm rõ các hạn chế của IPv4 và lý do cần chuyển đổi sang IPv6. Nội dung sẽ phân tích những lợi ích nổi bật của IPv6 như không gian địa chỉ mở rộng, hiệu suất cao hơn và khả năng hỗ trợ các công nghệ mới như 5G, IoT. Đồng thời, chương này cũng trình bày vai trò của các tổ chức quản lý tài nguyên Internet toàn cầu, đặc biệt là VNNIC trong thúc đẩy triển khai IPv6 tại Việt Nam.

CỤ THỂ, CHƯƠNG I SẼ CUNG CẤP CHO BẠN NHỮNG NỘI DUNG SAU:

Lịch sử phát triển của giao thức Internet từ IPv4 đến IPv6, bao gồm lý do ra đời của IPv6.

Các giải pháp tình thế được triển khai để hạn chế sự cạn kiệt của IPv4, như CIDR, VLSM, địa chỉ riêng và NAT.

Quá trình hình thành và phát triển của IPv6, bao gồm các đề xuất ban đầu và sự lựa chọn IPv6 với địa chỉ 128 bit.

Sự ra đời và vai trò của các tổ chức quản lý tài nguyên Internet toàn cầu (IANA, RIRs) trong việc cấp phát địa chỉ IP.

Vai trò của VNNIC trong việc quản lý tài nguyên Internet tại Việt Nam và thúc đẩy chuyển đổi sang IPv6.

Hiện trạng chuyển đổi sang IPv6 trên thế giới và tại Việt Nam, bao gồm các sự kiện quan trọng như World IPv6 Day và World IPv6 Launch.

Mối liên hệ và tầm quan trọng của IPv6 đối với các công nghệ hiện đại như mạng 5G và IoT.

Những lợi ích vượt trội của giao thức IPv6 so với IPv4.

Các phân vùng của không gian địa chỉ IPv6 và cách IANA phân bổ chúng cho các tổ chức khu vực.

1.1. VÀI NÉT LỊCH SỬ VỀ IPv4

Từ thập niên 1960, nhu cầu kết nối mạng cho các hệ thống máy tính với nhau đã xuất hiện. Đến những năm 1970, rất nhiều hệ thống mạng ra đời, trong đó đặc biệt nổi tiếng là mạng ARPANet của Mỹ, NPL của Anh, CYCLADES của Pháp. Tất cả các hệ thống mạng giai đoạn này đều sử dụng giao thức kết nối riêng và độc quyền. Điều này dẫn đến việc chia sẻ công việc và phối hợp nghiên cứu giữa các cơ quan, tổ chức bị hạn chế, vì thế rất nhiều giao thức liên mạng (Internetworking) được đề xuất và xây dựng trong suốt các thập niên 1980 và 1990 để kết nối các hệ thống mạng máy tính. Điều này dẫn đến những cuộc chiến giao thức (Protocol Wars) giữa những người làm kỹ thuật, các nhà nghiên cứu, các tổ chức và chính phủ nhiều nước, nhằm chọn ra giao thức mạng làm tiêu chuẩn chung cho việc truyền tải dữ liệu toàn cầu.

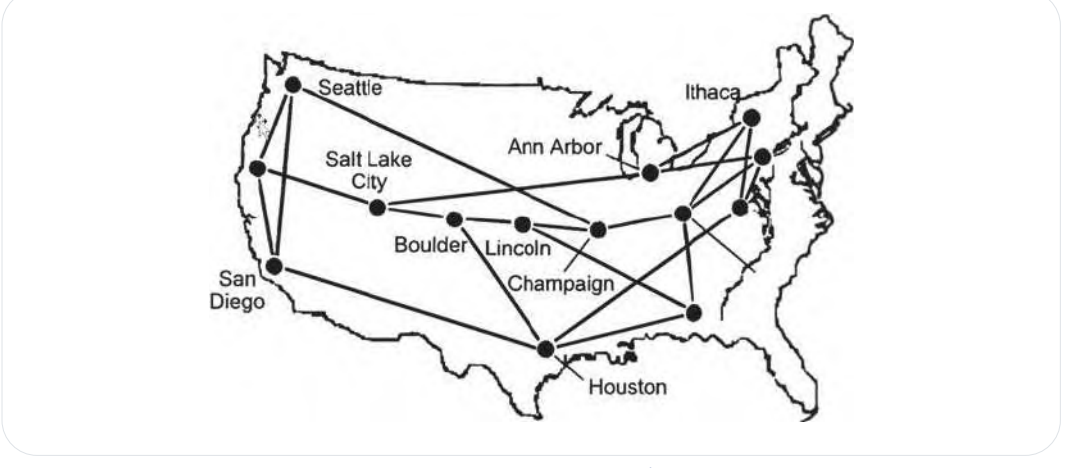
Bob Kahn và Vint Cerf là hai chuyên gia trong dự án "Xây dựng kiến trúc mở về kết nối liên mạng" (Open-architecture interconnection models) nhằm kết nối các hệ thống mạng của quân đội Mỹ, các trường đại học và viện nghiên cứu với hệ thống mạng của ARPANet (do cơ quan nghiên cứu ARPA quản lý). Vào tháng 12/1974 họ giới thiệu những mô tả đầu tiên về bộ giao thức Internet Protocol trong RFC 675, sau đó bộ giao thức này được thử nghiệm và thay đổi rất nhiều lần từ phiên bản 1 đến 3. Đến tháng 9/1981, phiên bản 4 của bộ giao thức TCP/IP được công bố chính thức trong **RFC 791** (dành cho giao thức IP) và **RFC 793** (dành cho giao thức TCP). Đây là phiên bản rất thành công và còn được dùng phổ biến hiện nay.

Bộ giao thức TCP/IP từ khi được giới thiệu chính thức đã gây được tiếng vang lớn bởi vì nó đại diện cho một kiến trúc mở (open-architecture), không bản quyền (royalty-free) và không độc quyền (non-proprietary). Nó cho phép bất kỳ loại máy tính nào cũng có thể giao tiếp với nhau thông qua bất kỳ môi trường truyền dẫn nào. Ngoài ra TCP/IP chỉ đơn giản là thành phần phần mềm được cài đặt trên các máy tính nên khả năng triển khai nhanh chóng và dễ dàng tương thích những hệ thống mạng hiện có.

Ngày 01/01/1983 được coi là "ngày giương cờ" (Flag day) của bộ giao thức TCP/IP khi toàn bộ mạng ARPNet chính thức chuyển sang sử dụng chuẩn này (theo hướng dẫn của RFC 801 trước đó). Tuy nhiên, phải hơn một thập kỷ sau, đến giữa những năm 1990, bộ giao thức này mới thực sự chiếm ưu thế toàn cầu và trở thành tiêu chuẩn phổ biến.

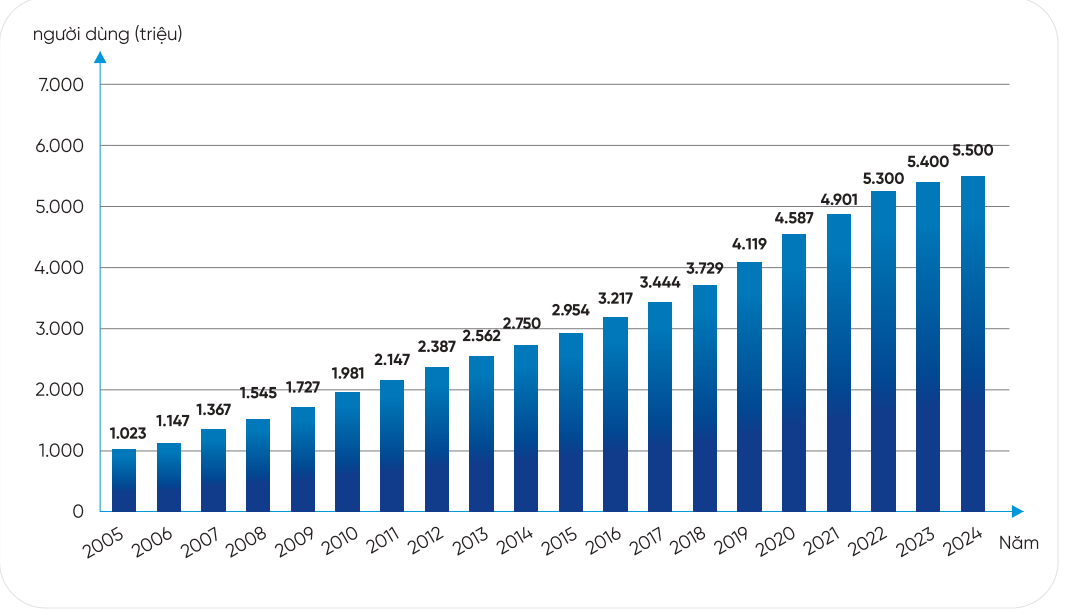
1.2. LỊCH SỬ PHÁT TRIỂN CỦA MẠNG INTERNET

Năm 1986, mạng NSFNet (National Science Foundation Network) ra đời nhằm kết nối các trung tâm siêu máy tính (Supercomputer center) và các trường đại học tại Mỹ. Đến năm 1989, NSFNet có khoảng 1000 hệ thống mạng kết nối (theo RFC 1118) với 3 triệu người dùng.



Hình 1. Mạng NSFNet năm 1991 (nguồn: Internet)

Đây được coi như là mạng trục đầu tiên của Internet. Sang năm 1993, mạng Internet bắt đầu lan ra quy mô toàn cầu. Cùng lúc đó công nghệ kết nối Internet Dial-up được thương mại hóa năm 1992, rồi các công nghệ băng rộng (Broadband) lần lượt ra đời, kết hợp với mạng WWW (World Wide Web), máy tính cá nhân ... Tất cả những điều này thực sự khiến cho mạng Internet bùng nổ. Lúc này các chuyên gia Internet đã bắt đầu nhận ra vấn đề của IPv4, RFC 1287 vào tháng 12/1991 đã dự đoán có thể có đến 10^7-10^{10} hệ thống mạng sẽ kết nối Internet, đồng nghĩa không gian địa chỉ IPv4 sẽ bị cạn kiệt.



Hình 2. Số lượng người dùng Internet qua các năm (nguồn: www.statista.com)

1.3. CÁC GIẢI PHÁP TÌNH THẾ CHO VẤN ĐỀ CỦA IPv4

Từ năm 1992, các chuyên gia và tổ chức đã bắt đầu thảo luận về giải pháp thay thế IPv4. Năm 1993, IETF kêu gọi đề xuất cho thế hệ giao thức IP mới mang tên IPng. Đến năm 1994, IETF thống nhất sử dụng địa chỉ IP dài 128 bit (RFC 1752) và đặt tên chính thức là IPv6 trong RFC 1883.

Trong bối cảnh Internet phát triển mạnh, mang lại lợi ích lớn cho nhà cung cấp dịch vụ, nội dung, thiết bị và hạ tầng mạng, việc chuyển đổi sang IPv6 bị xem là rủi ro do có thể ảnh hưởng đến dịch vụ và doanh thu hiện tại. Do đó, nhiều giải pháp đã được triển khai nhằm làm chậm quá trình cạn kiệt của địa chỉ IPv4 trong khi tiếp tục đầu tư, chuyển đổi sang giao thức thế hệ mới. Một số giải pháp này rất thành công trong việc tối ưu sử dụng địa chỉ IPv4 và hỗ trợ quá trình chuyển đổi sang IPv6:

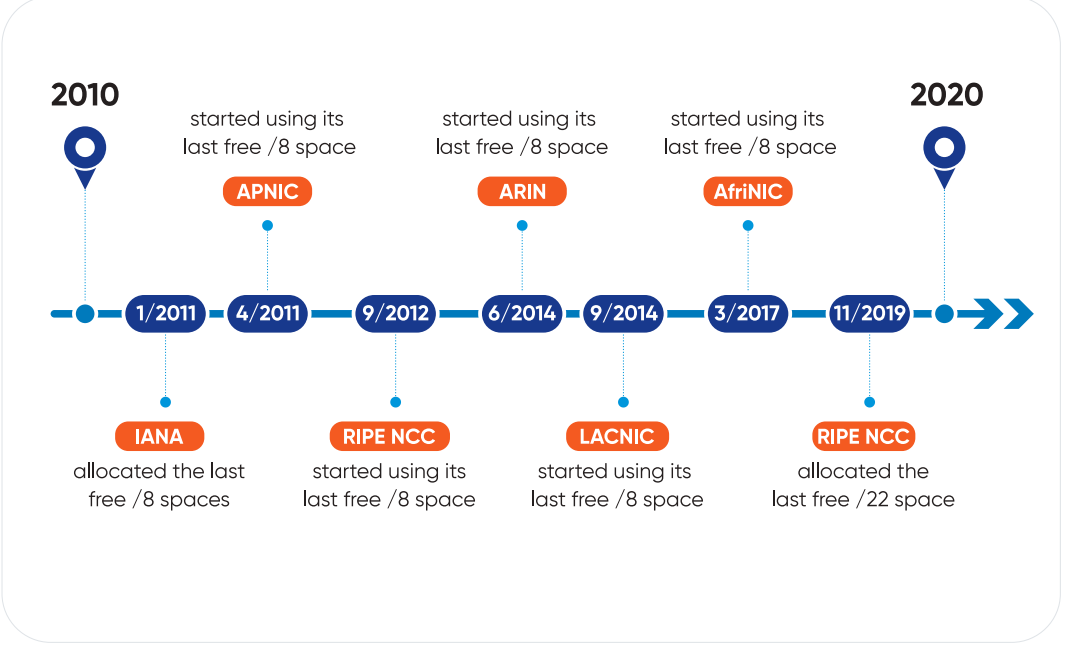
- **RFC 1519** (9/1993): Kỹ thuật **CIDR** (Classless Inter-Domain Routing) đã xóa ý nghĩa của việc phân chia địa chỉ IPv4 thành các lớp mặc định A, B, C ...thay vào đó cho phép gom các lớp địa chỉ này thành các dãy mạng lớn hơn gọi là Supernet. Việc này giúp cho việc phân bổ địa chỉ IPv4 hiệu quả hơn, ví dụ cho phép cấp các dãy địa chỉ /14, /15 thay vì /8 hoặc /20, /23 thay cho /16. Đặc biệt kỹ thuật này giúp bảng định tuyến (Routing table) toàn cầu gọn hơn, giảm yêu cầu bộ nhớ và tăng tốc độ xử lý trên các thiết bị định tuyến.
- **RFC 1878** (10/1993): Kỹ thuật **VLSM** (Variable Length Subnet Mask) dựa trên cơ sở của CIDR cho phép chia một dãy mạng được cấp thành những mạng con nhỏ hơn (Subnet) nhằm tối ưu trong việc phân chia địa chỉ trong các hệ thống mạng, giúp tiết kiệm địa chỉ khi phân bổ những hệ thống có số lượng máy tính nhỏ.

- **RFC 1597** (3/1994): Đây là giải pháp rất hiệu quả, trong đó quy định những dãy địa chỉ nội bộ **(Private IP address)** mà các tổ chức, doanh nghiệp không có nhu cầu kết nối Internet có thể sử dụng mà không cần xin phép hay đăng ký. Các dãy địa chỉ này không có ý nghĩa trên Internet và được dùng lại giữa các mạng nội bộ. RFC này được cập nhật thay thế bằng RFC 1918 sau này và thường được nêu trong các tài liệu thay vì tên RFC 1597.

- **RFC 1631** (5/1994): Có thể nói **NAT** (Network Address Translator) là giải đột phá nhất, nó cho phép ánh xạ một hay nhiều địa chỉ Private thành một địa chỉ Public. Điều này giúp việc sử dụng địa chỉ IP Public hiệu quả hơn, hạn chế tối đa tình trạng cạn kiệt địa chỉ IPv4. Một giải pháp bổ sung khác là kỹ thuật **CGNAT** (Carrier-grade NAT) được mô tả trong RFC 6598 (4/2012) cho phép thực hiện NAT lần 2 tại các nhà mạng giúp tiết kiệm thêm lần nữa.

- **RFC 1541** (10/1993): Một giải pháp ít được nhắc đến đó là **DHCP** (Dynamic Host Configuration Protocol). Giao thức này dựa trên nền tảng của giao thức BOOTP nhưng điều khác biệt là BOOTP gán địa chỉ IP tự động nhưng địa chỉ đó không thay đổi sau các lần gán trong khi DHCP cũng cấp tự động nhưng là địa chỉ ngẫu nhiên mỗi lần gán. Việc này cho phép các nhà mạng thu hồi địa chỉ IP còn trống để gán cho máy tính khác nên sẽ giúp tăng hiệu quả sử dụng dãy địa chỉ IP.

Dù nhiều giải pháp tiết kiệm đã được áp dụng, nguồn địa chỉ IPv4 dự trữ trên toàn cầu của IANA đã chính thức cạn kiệt vào ngày 03 tháng 02 năm 2011, khi dãy /8 cuối cùng được phân bổ cho các Regional Internet Registries (RIR). Sau đó, các RIR tiếp tục quản lý và phân bổ địa chỉ còn lại, nhưng đến những năm sau, hầu hết các khu vực cũng đã bắt đầu sử dụng nguồn dự phòng cuối cùng của mình để phân bổ.



Hình 3. Quá trình cạn kiệt địa chỉ IPv4 của các tổ chức quản lý tài nguyên cấp vùng (nguồn: Wikipedia)

1.4. CÂU CHUYỆN RA ĐỜI CỦA IPv6

Tổ chức **Internet Architecture Board (IAB)** được thành lập năm 1983 với vai trò định hướng kỹ thuật dài hạn cho sự phát triển của Internet, bảo đảm Internet tiếp tục mở rộng và đổi mới như một nền tảng truyền thông toàn cầu (RFC 1120). Nhằm hỗ trợ xây dựng các giao thức và tiêu chuẩn mạng, **IETF (Internet Engineering Task Force)** được thành lập năm 1986 như một tổ chức trực thuộc IAB. IETF chịu trách nhiệm phát triển các tiêu chuẩn kỹ thuật, trong khi IAB giám sát, định hướng và đảm bảo sự phù hợp với kiến trúc tổng thể của Internet.

Trong thập niên 1970–1980, nhiều giao thức mạng được phát triển như SNA, X.25, TCP/IP, IPX/SPX, AppleTalk... nhưng chưa có giao thức nào nổi trội tuyệt đối. Đồng thời, **ISO** – tổ chức tiêu chuẩn quốc tế thành lập từ năm 1947 – đã đóng vai trò lớn trong việc xây dựng tiêu chuẩn công nghệ, đối với lĩnh vực mạng máy tính, năm 1984 ISO giới thiệu **mô hình tham chiếu 7 lớp OSI**, được dùng phổ biến đến ngày nay. ISO và ITU cũng phát triển bộ giao thức mạng theo mô hình OSI, tuy nhiên bộ giao thức này không tương thích với TCP/IP – giao thức sau đó trở thành nền tảng chính của Internet toàn cầu.

<table>
<tr><td rowspan="2">7</td><td>FTAM
ISO 8571</td><td colspan="2">CMISE
ISO 9596
ISO 9595</td><td rowspan="2">Application</td></tr>
<tr><td>ACSE
X.227, ISO 8650
X.217, ISO 8649</td><td colspan="2">ACSE
X.227, ISO 8650
X.217, ISO 8649
ROSE
ISO 9072,
X.219, X.229</td></tr>
<tr><td>6</td><td colspan="3">X.226, ISO 8823
X.209, ISO 8825 BER
X.216, ISO 8822</td><td>Presentation</td></tr>
<tr><td>5</td><td colspan="3">X.225, ISO 8327
X.215, ISO 8326</td><td>Session</td></tr>
<tr><td>4</td><td colspan="3">X.224, ISO 8073 / AD 2
(X.214, ISO 8072 / AD 2)
Class 4</td><td>Transport</td></tr>
<tr><td rowspan="2">3</td><td colspan="3">ISO 9542 (ES-IS)
ISO 10589 (IS-IS Level 1) / ISO 10747 (IS-IS Level 2)</td><td rowspan="2">Network</td></tr>
<tr><td>ISO 8473-3 (CLNS)
ISO 8208 X.25 Packet Level</td><td>ISO 8473-2
(CLNS)</td><td>ISO 8473-4
(CLNS)</td></tr>
<tr><td>2</td><td>ISO 7776 LapB
X.25 Data Link Layer</td><td>ISO 802.2 LLC
ISO 802.3 MAC</td><td>Q.921 LapD</td><td>Data Link</td></tr>
<tr><td>1</td><td>X.21 / X.21bis
V.35 / G.703
2M TS n</td><td>ISO 802.2 Ethernet</td><td>SDH-DCC 2M TS n</td><td>Physical</td></tr>
</table>

Hình 4. Chi tiết ISO Protocol Stack
(nguồn: http://www.cellsoft.de/telecom/dcn.htm)

Bộ giao thức **OSI** từng nhận được sự ủng hộ mạnh mẽ từ các nhà cung cấp viễn thông lớn, nhiều chính phủ của các nước châu Âu (đặc biệt là Pháp, Tây Đức, Anh, Cộng đồng Kinh tế châu Âu) và cả Bộ Thương mại Mỹ. Năm 1988, **Bộ Quốc phòng Mỹ** từng lên kế hoạch chuyển đổi từ TCP/IP sang OSI. Điều này góp phần tạo nên **"cuộc chiến giao thức"** (Protocol Wars), mà đỉnh điểm là sự cạnh tranh gay gắt giữa TCP/IP và OSI.

Tuy nhiên, sự xuất hiện của **World Wide Web (WWW)** vào năm 1990 đã thúc đẩy Internet phát triển mạnh mẽ. Với sự hỗ trợ của các nhà sản xuất thiết bị mạng, TCP/IP nhanh chóng chiếm ưu thế và được lựa chọn làm nền tảng của mạng Internet. Đến năm 1994, **Chính phủ Mỹ chính thức tuyên bố sử dụng TCP/IP cho toàn bộ hệ thống mạng**, chấm dứt yêu cầu tương thích với giao thức OSI.

**Chú ý: Xem thêm nội dung liên quan tại: https://en.wikipedia.org/wiki/Protocol_Wars*

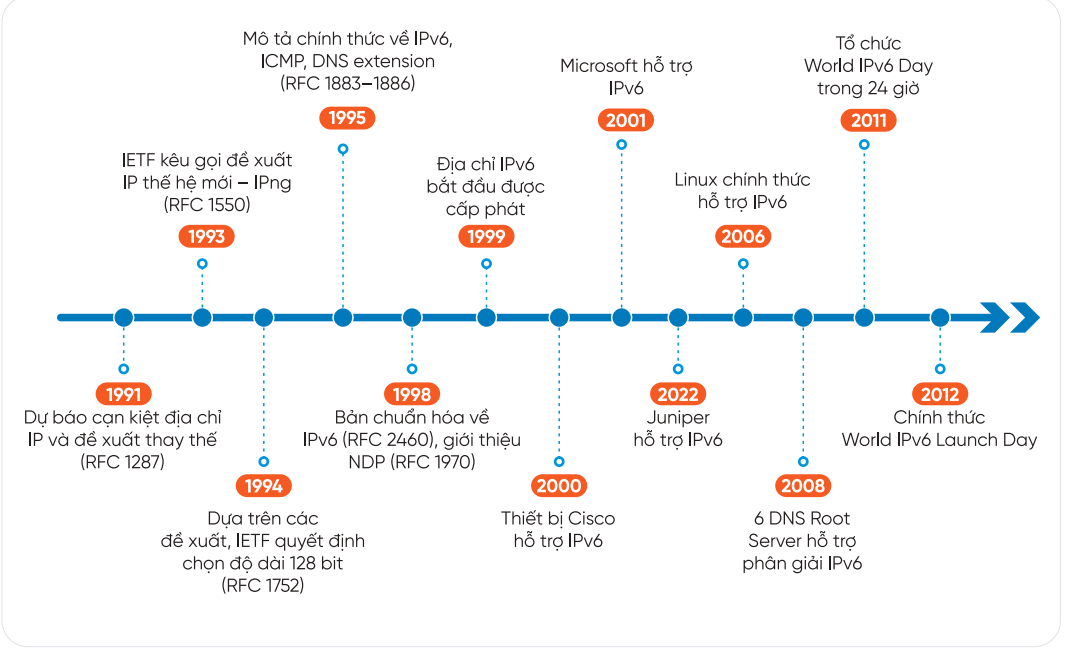
Ngay từ những năm 1990, các chuyên gia đã dự báo nguy cơ cạn kiệt địa chỉ IPv4 – khi đó web vẫn chưa xuất hiện và các kỹ thuật như NAT, DHCP, CIDR hay VLSM vẫn chưa ra đời. Năm 1991, trong RFC 1287, IETF đã mô tả chi tiết sự cạn kiệt này, nhận định khả năng tồn tại đồng thời cả 2 giao thức TCP/IP và OSI và đề xuất xây dựng thế hệ địa chỉ IP mới.

Tháng 6/1992, đại diện IAB tham dự cuộc họp tại Nhật Bản do ISOC tổ chức và đồng thuận xem xét áp dụng giao thức TUBA (TCP and UDP with Bigger Addresses) thay thế IPv4. TUBA là giao thức phát triển từ giao thức CLNP (Connectionless Network Protocol) thuộc bộ giao thức OSI, có độ dài 160 bit nhưng cho phép các giao thức tầng ứng dụng và TCP/UDP chạy trên nền của CLNP. TUBA được dự định đặt tên là IPv7, bỏ qua cả tên gọi IPv6.

Tuy nhiên, cộng đồng IETF không đồng tình việc này. Năm 1993, họ đã kêu gọi các đề xuất cho giao thức mới có tên gọi IPng (IP next generation) thay thế cho IPv4 trong RFC 1550. Có 3 giao thức chính được đề xuất giai đoạn này:

- **CATNIP (Common Architecture for the Internet):** Hỗ trợ đồng thời cả 3 giao thức IPv4, IPX và CLNP.
- **TUBA (TCP/UDP over CLNP-Addressed Networks):** Sử dụng địa chỉ 160 bit và định dạng gói tin theo giao thức CLNP của OSI.
- **SIPP (Simple Internet Protocol Plus):** Đề xuất nâng cấp giao thức IPv4 lên 64 bit, thay đổi định dạng bản tin IPv4 và bổ sung một số tính năng mới vào IPv4.

Năm 1994, IETF đã thống nhất lựa chọn giải pháp SIPP với chiều dài của địa chỉ IP thế hệ mới là 128 bit và đặt tên gọi mới là IPv6 thay cho IPng.



Hình 5. Lịch sử ra đời của IPv6 và các giao thức, hoạt động hỗ trợ

Tiếp theo, năm 1995 IETF đã giới thiệu chính thức và mô tả chi tiết giao thức IPv6 trong RFC 1883. Giao thức này sau quá trình triển khai đánh giá thực tế đã được cập nhật bằng RFC 2460 năm 1998.

1.5. CÁC PHIÊN BẢN IP KHÁC Ở ĐÂU?

Ban đầu, mạng ARPANET sử dụng giao thức **NCP (Network Control Program)** để truyền dữ liệu, nhưng NCP không đáp ứng được nhu cầu mở rộng mạng quy mô lớn. Trước yêu cầu kết nối ARPANET với mạng của các trường đại học và viện nghiên cứu tại Mỹ, ARPA đã đề xuất xây dựng giao thức mới có tên **Transmission Control Program**, được mô tả trong **RFC 675** và thử nghiệm lần đầu vào năm 1974 với 2 node mạng, sau đó là 3 node vào năm 1977.

Đến năm 1978, giao thức này được tách thành 2 phần: **TCP (Transmission Control Protocol)** và **IP (Internet Protocol)**. Sau 2 giai đoạn thử nghiệm và hoàn thiện, năm 1981, bộ giao thức TCP/IP chính thức được công bố trong **RFC 791** (cho IP) và **RFC 793** (cho TCP). Bộ giao thức này được đặt tên là **phiên bản 4 (IPv4)**, dù các phiên bản 1 đến 3 chưa từng được đặt tên hoặc ban hành chính thức.

PHIÊN BẢN	TÊN GỌI	CỘT MỐC THỜI GIAN
0-3		Không được gán
Giới thiệu	Transmission Control Program	Được Vint Cerf and Bob Kahn giới thiệu vào tháng 12/1974 theo RFC 675
Thử nghiệm	TCP lần 1	Năm 1975
	TCP lần 2	Năm 1977
	Tách thành hai giao thức TCP và IP	Năm 1978
4	TCPv4/IPv4	• TCPv4: RFC 793 vào tháng 9/1981 • IPv4: RFC 791 vào tháng 9/1981 • Đây là phiên bản thành công nhất và vẫn còn được sử dụng phổ biến đến bây giờ
5	IPv5	Đặt tên cho giao thức Internet Stream Protocol nhằm tối ưu việc truyền dữ liệu Video được mô tả trong RFC 1190 vào tháng 11/1990 nhưng chỉ là đề xuất, không được nghiên cứu và áp dụng
6	IPv6	RFC 1883 vào tháng 12/1995 là mô tả chính thức giao thức này

Bảng 1. Tóm tắt các phiên bản của giao thức Internet Protocol

IPv5 không phải là một phiên bản IP chính thức, mà là tên được dùng cho **Internet Stream Protocol** – một đề xuất thuộc tầng mạng nhằm hỗ trợ truyền tải đa phương tiện có đảm bảo chất lượng dịch vụ (QoS). Giao thức này được mô tả trong **RFC 1190 (1990)** và **RFC 1819 (1995)**, nhưng chỉ dừng lại ở mức thử nghiệm, không được triển khai rộng rãi.

Dù vậy, **IETF** vẫn gán số hiệu **IPv5** cho đề xuất này và do đó, phiên bản tiếp theo của IPv4 được đặt tên là **IPv6**. Ngoài ra, từng có đề xuất IPv7 cho giao thức **TUBA**, nhưng đây chỉ là thảo luận nội bộ, chưa bao giờ trở thành tiêu chuẩn.

1.6. ĐỊA CHỈ IPv6 NHIỀU NHƯ THẾ NÀO?

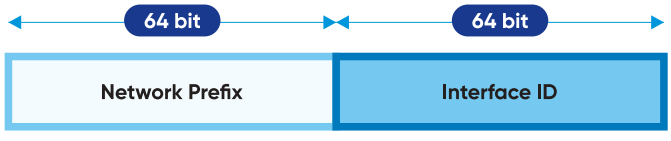
IPv6 ra đời nhằm giải quyết sự cạn kiệt của địa chỉ IPv4, chính vì thế IPv6 được thiết kế sẽ không lặp lại vấn đề của IPv4, điều này có nghĩa là IPv6 sẽ không bao giờ bị cạn kiệt lần nữa như đối với IPv4. Như vậy chắc chắn rằng không gian địa chỉ của IPv6 rất lớn và làm sao để hình dung được khả năng này?

Với độ dài 128 bit thì số lượng địa chỉ IPv6 sẽ là:

2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456 (39 chữ số)

Nếu phân chia theo bề mặt trái đất thì mỗi mét vuông mặt đất sẽ có $6{,}65 \times 10^{23}$ địa chỉ. Có người còn cho rằng mỗi hạt cát trên trái đất nếu được cấp nhiều địa chỉ IPv6 thì vẫn đủ.

Nếu bạn vẫn chưa hình dung được thì có cách tính dễ hiểu hơn như sau. Địa chỉ IPv6 Global Unicast được quy định trong RFC 2373 gồm có hai phần đều bằng 64 bit: Network Prefix đại diện cho mạng và Interface ID đại diện cho một máy tính trên mạng đó.



Hình 6. Cấu trúc địa chỉ IPv6 Global Unicast

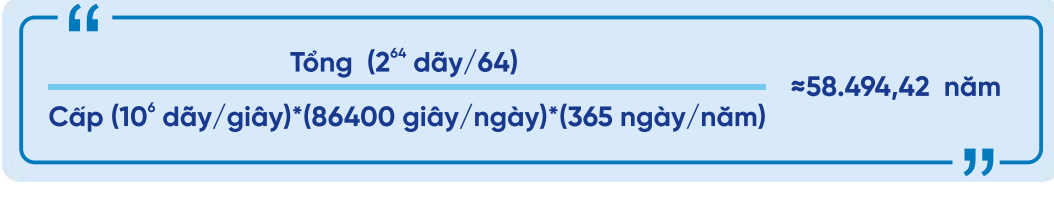
Như vậy chiều dài của phần Network Prefix dài nhất là /64, với 64 bit thì tổng số lượng dãy Network Prefix của IPv6 là:

2^{64}= 18.446.744.073.709.551.616 (18 tỷ tỷ) dãy

Giả sử phân bổ 10.000.000 (10 triệu) Network Prefix /64 mỗi giây thì số năm để phân bổ hết sẽ được tính như sau:

- Mỗi năm có: 365 * 24 * 60* 60 = 31.536.000 giây
- Mỗi năm cấp được: 10.000.000 * 31.536.000 = 315.360.000.000.000
- Để cấp hết toàn bộ Network Prefix /64 thì cần:

  18.446.744.073.709.551.616 / 315.360.000.000.000 = 58.494,24 năm



Hình 7. Minh họa số lượng địa chỉ IPv6

Như vậy, cần đến hơn 58.000 năm để cấp hết số lượng Network Prefix /64 với tốc độ cấp là 10 triệu Network Prefix mỗi giây, nên có thể nói rằng địa chỉ IPv6 rất khó bị cạn kiệt một lần nữa hay có thể coi là gần như vô hạn. Đây là sự khác biệt quan trọng của IPv6 so với IPv4, vì thế một số quan niệm cũ như tính toán tiết kiệm khi phân chia mạng con theo số lượng máy hiện có, các kỹ thuật VLSM... không còn được dùng trong IPv6.

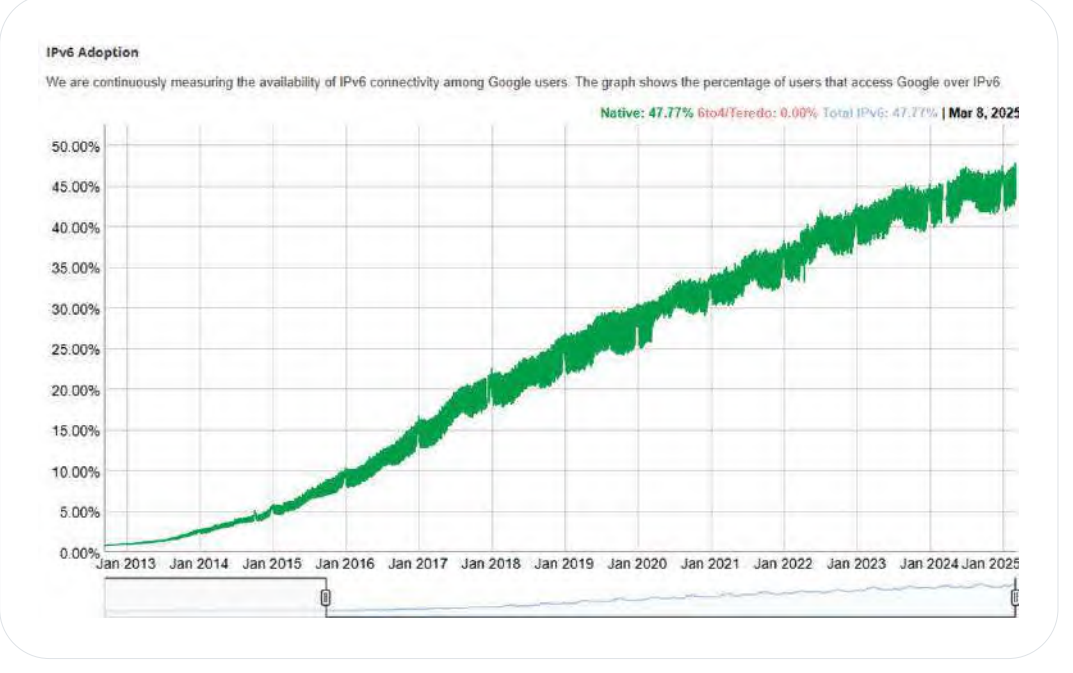
1.7. HIỆN TRẠNG CHUYỂN ĐỔI SANG IPv6 TRÊN THẾ GIỚI

Sau khi được chuẩn hóa trong **RFC 2460 (1998)**, **IPv6** bắt đầu được cấp phát cho các **RIR** từ năm 1999. Nhiều tổ chức đã tiên phong thử nghiệm như **KAME, 6Bone, 6Net, GEANT**... nhằm đánh giá tính năng và khả năng hoạt động của IPv6.

Tuy nhiên, **việc triển khai thực tế diễn ra rất chậm**, chủ yếu do sự hiệu quả của các kỹ thuật tiết kiệm địa chỉ IPv4 như NAT, CIDR, DHCP... khiến các **nhà mạng** và **nhà cung cấp nội dung** chưa mặn mà với IPv6.

Để thúc đẩy chuyển đổi, ngày **08/6/2011**, **ISOC** tổ chức sự kiện **"World IPv6 Day"** kéo dài 24 giờ, với sự tham gia của hơn 400 tổ chức với hơn 1000 Website nội dung lớn nhất toàn cầu. Mục tiêu là kiểm tra tính ổn định khi chạy song song IPv6 và IPv4, qua đó phát hiện và xử lý các vấn đề tiềm ẩn.

Thành công của sự kiện đã tạo đà cho **"World IPv6 Launch"** vào **ngày 06/6/2012**, đánh dấu việc **chính thức triển khai IPv6** trên toàn cầu. Đây là **cột mốc quan trọng**, khẳng định **khả năng hiện thực của IPv6** và mở ra **kỷ nguyên Internet thế hệ mới.**



Hình 8. Tỉ lệ người dùng IPv6 qua các năm (nguồn: Google)

Trong giai đoạn từ năm 2011 đến năm 2015, tỉ lệ người sử dụng IPv6 toàn cầu tăng từ gần 0% lên 5%. Sau đó, chỉ cần 3 năm từ năm 2015 đến năm 2018, tỉ lệ này tăng rất nhanh từ 5% lên đến 20%. Từ năm 2018 đến nay, tỉ lệ tăng trưởng vẫn ở mức cao. Đầu tháng 3/2025, tỉ lệ người dùng IPv6 toàn cầu đã đạt gần 48%.

1.8. NHỮNG CỘT MỐC TRIỂN KHAI IPv6 TẠI VIỆT NAM VÀ MỤC TIÊU IPv6 ONLY

Hành trình chuyển đổi sang giao thức IPv6 tại Việt Nam đã được khởi động từ rất sớm, với những cột mốc quan trọng đánh dấu sự quyết tâm của Chính phủ trong việc xây dựng một hạ tầng Internet hiện đại, bền vững, sẵn sàng cho các công nghệ mới.

Ngày 06/5/2008

Bộ trưởng Bộ Thông tin và Truyền thông ban hành Chỉ thị số 03/2008/CT-BTTTT, chính thức khởi động quá trình thúc đẩy sử dụng địa chỉ Internet thế hệ mới IPv6. Đây là bước đi quan trọng nhằm thay thế nguồn IPv4 đã cạn kiệt, đảm bảo sự phát triển bền vững của Internet Việt Nam.

Ngày 06/01/2009

Cột mốc quan trọng với sự thành lập của "Ban Công tác thúc đẩy phát triển IPv6 quốc gia" do Thứ trưởng Bộ TT&TT là Trưởng ban, Trung tâm Internet Việt Nam (VNNIC) là Thường trực Ban theo Quyết định số 05/QĐ-BTTTT.

Ngày 29/3/2011

Một bước tiến lớn được ghi nhận khi Bộ trưởng Bộ Thông tin và Truyền thông ký ban hành Kế hoạch hành động quốc gia về IPv6 (theo Quyết định số 433/QĐ-BTTTT, được sửa đổi bổ sung tại Quyết định số 1509/QĐ-BTTTT ngày 20/10/2014). Kế hoạch này triển khai từ năm 2011 đến năm 2019, với mục tiêu rõ ràng: "Internet Việt Nam hoạt động an toàn, tin cậy với địa chỉ IPv6 kể từ năm 2019".

Ngày 06/5/2013

Một bước đột phá về chuyển đổi IPv6 khi VNNIC tổ chức Lễ khai trương IPv6 Việt Nam. Tại sự kiện này, VNNIC phối hợp với các doanh nghiệp cung cấp dịch vụ Internet lớn (VNPT, Viettel, FPT Telecom, NetNam, VTC...) chính thức đưa vào vận hành mạng IPv6 quốc gia. Hệ thống này được xây dựng trên cơ sở kết nối song song IPv4/IPv6, bao gồm hệ thống DNS quốc gia, trạm trung chuyển Internet quốc gia VNIX và mạng Internet của các doanh nghiệp cung cấp dịch vụ Internet.

Ngày 14/01/2021

Để đẩy mạnh ứng dụng IPv6 trong các cơ quan nhà nước, Bộ trưởng Bộ Thông tin và Truyền thông phê duyệt "Chương trình thúc đẩy, hỗ trợ chuyển đổi IPv6 cho cơ quan nhà nước giai đoạn 2021 - 2025" (Quyết định số 38/QĐ-BTTTT). Đây là bước đi chiến lược nhằm đảm bảo các cơ quan nhà nước tiên phong trong việc ứng dụng IPv6 trên mạng lưới và dịch vụ.

Tiêu chuẩn công nghệ về IPv4 đã dừng phát triển từ tháng 11/2016 (Ủy ban kiến trúc Internet IAB công bố). Các tiêu chuẩn mới cho IPv6, IPv6 Only đã được hoàn thiện, ứng dụng rộng rãi để phát triển Internet thế hệ mới, Internet công nghiệp, IoT, Cloud, 5G, 6G... IPv6 là yếu tố cơ bản, thiết yếu của hạ tầng Internet, hạ tầng số, các dịch vụ số, dựa trên ứng dụng công nghệ IPv6 có thể sáng tạo, tạo ra nhiều giá trị mới.

> **Chuyển đổi IPv6 là xu thế tất yếu để phát triển Internet vạn vật, Internet công nghiệp với các dịch vụ mới như IoT, Cloud Computing, 5G/6G.**

65,5% tỷ lệ sử dụng IPv6
Tính đến tháng 12/2024 tại Việt Nam

Top 2 Đông Nam Á
Top 7 Toàn cầu

Tăng 2 bậc so với năm 2023 (gấp 1,6 lần bình quân toàn cầu, đứng trên Mỹ, Trung Quốc, Nhật Bản, Hàn Quốc, Anh, Pháp).

100%
Hạ tầng Internet quan trọng quốc gia hoạt động với IPv6 (DNS, VNIX).

Hình 9. Công bố của VNNIC về tỷ lệ người dùng IPv6 tại Việt Nam (nguồn: Báo cáo tài nguyên Internet năm 2024)

Tỉ lệ chuyển đổi IPv6 của Việt Nam đã đạt cột mốc rất ấn tượng, liên tục đứng trong Top 10 của thế giới.

Cuối năm 2024

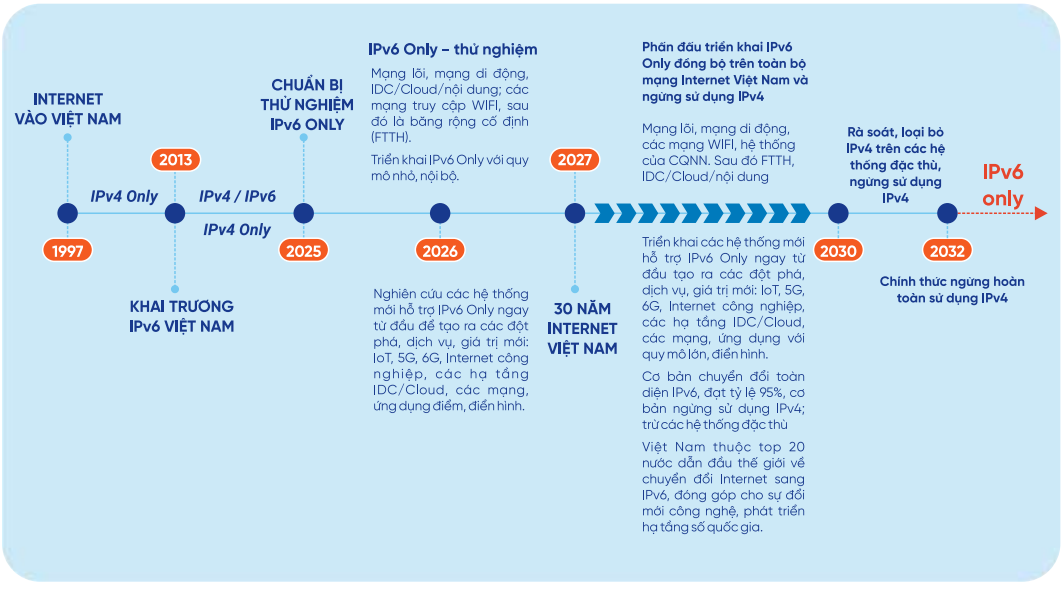
Tỉ lệ người dùng IPv6 tại Việt Nam đạt 65,5%, vượt xa mức trung bình 48% của thế giới, đưa Việt Nam đứng thứ 7 trên toàn cầu và thứ 2 khu vực ASEAN. Có thể thấy số lượng người dùng IPv6 tại Việt Nam đã vượt rất xa số người dùng thuần IPv4.

Mục tiêu 2025

Việt Nam đặt mục tiêu đạt tỉ lệ sử dụng IPv6 70%, giữ vững vị trí trong top 10 toàn cầu, theo Nghị quyết số 01/NQ-CP ngày 08/01/2025 của Chính phủ và Chỉ thị số 01/CT-BTTTT ngày 15/01/2025 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ). Chương trình IPv6 For Gov giai đoạn 2021-2025 sẽ hoàn thành với 100% cổng thông tin điện tử, dịch vụ công cơ quan nhà nước sử dụng IPv6, mạng truyền số liệu chuyên dùng hoạt động ổn định và sẵn sàng vận hành thuần IPv6. Đồng thời, IPv6 Only được thử nghiệm trong khối cơ quan nhà nước, cùng với việc nghiên cứu và xây dựng lộ trình chuyển đổi IPv6 Only cho giai đoạn tiếp theo.

Giai đoạn 2026-2032

Để bắt kịp xu hướng của thế giới, VNNIC đã đề xuất lộ trình chuyển đổi sang IPv6 Only, bắt đầu thử nghiệm từ năm 2026 và tắt hoàn toàn IPv4, chỉ sử dụng IPv6 Only từ năm 2032.

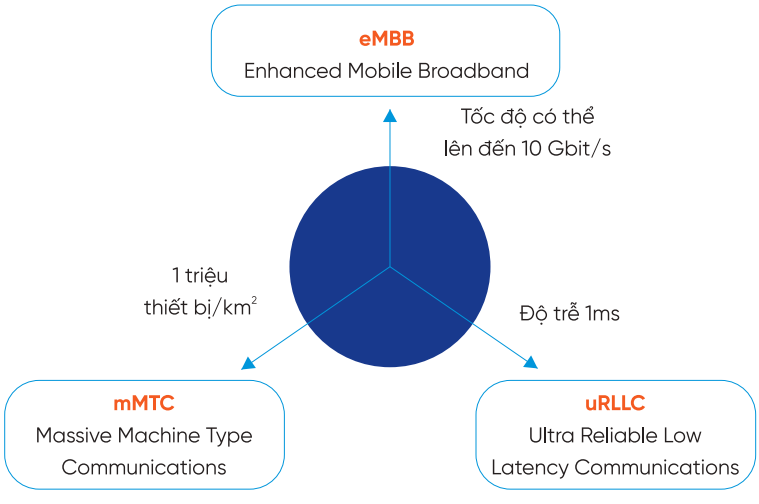


Hình 10. Lộ trình dự kiến tắt IPv4 chuyển sang IPv6 Only từ VNNIC

Kế hoạch ngừng sử dụng IPv4 để chuyển đổi toàn diện sang IPv6 của Việt Nam không chỉ giải quyết vấn đề hạn chế về không gian địa chỉ mà còn là một chiến lược quan trọng để xây dựng hạ tầng số hiện đại và bền vững. Đây là cơ hội để khẳng định vị thế công nghệ của Việt Nam trên trường quốc tế, đồng thời đặt nền móng cho sự phát triển lâu dài của hệ sinh thái mạng, sẵn sàng cho các công nghệ tiên tiến như IoT và 5G.

1.9. VAI TRÒ CỦA IPv6 VỚI MẠNG 5G

IPv6 và mạng di động 5G được xem là hai yếu tố quan trọng định hình tương lai của Internet, mang đến sự đột phá về tốc độ, độ trễ thấp và khả năng kết nối hàng loạt thiết bị. Với yêu cầu kỹ thuật cao của 5G, IPv6 đáp ứng hoàn hảo nhờ không gian địa chỉ rộng, tính linh hoạt cao và hiệu quả hoạt động tối ưu. Chính vì thế, sự phát triển của 5G sẽ là động lực thúc đẩy quá trình chuyển đổi sang IPv6, đưa Internet tiến gần hơn đến một mô hình mạng toàn diện, thông minh và tối ưu, hiệu quả hơn.



Hình 11. Các đặc trưng của mạng 5G

Triển khai 5G: Từ NSA đến SA

Trong lộ trình phát triển mạng di động thế hệ mới, 5G được triển khai trên toàn cầu qua hai giai đoạn chính: 5G phụ thuộc (NSA – Non-Standalone) và 5G độc lập (SA – Standalone). Hai mô hình này không chỉ khác biệt về mặt kiến trúc mà còn thể hiện mức độ trưởng thành và năng lực thực tế của mạng 5G.

5G NSA là giai đoạn đầu tiên, nơi các nhà mạng tận dụng hạ tầng mạng truy nhập vô tuyến (RAN) và mạng lõi (Core Network) của 4G LTE hiện có để cung cấp dịch vụ 5G. Mô hình này giúp giảm chi phí đầu tư ban đầu, tận dụng thiết bị và vùng phủ sóng sẵn có, đồng thời rút ngắn thời gian triển khai. Tuy nhiên, 5G NSA chủ yếu cải thiện tốc độ truyền dữ liệu (phục vụ nhu cầu eMBB – enhanced Mobile Broadband), hướng đến các thiết bị như điện thoại thông minh và máy tính bảng. Hạn chế lớn của mô hình này là không đáp ứng được các yêu cầu khắt khe hơn của 5G thực thụ, như độ trễ siêu thấp (uRLLC) hay khả năng kết nối đồng thời hàng loạt thiết bị (mMTC). Do đó, NSA được xem như một bước chuyển tiếp, chưa thể khai thác hết tiềm năng của 5G.

Ngược lại, 5G SA đại diện cho tầm nhìn đầy đủ của mạng 5G. Với kiến trúc mạng lõi được thiết kế mới hoàn toàn, độc lập với hạ tầng 4G, 5G SA không chỉ cung cấp tốc độ vượt trội mà còn hỗ trợ đa dạng các kịch bản ứng dụng: từ Internet vạn vật (IoT), thành phố thông minh, đến công nghiệp 4.0 và phương tiện tự hành. Kiến trúc độc lập này cho phép tối ưu hóa mạng, giảm độ trễ xuống dưới 1ms trong điều kiện lý tưởng, đồng thời mở rộng khả năng kết nối hàng tỷ thiết bị thông minh.

Điểm đáng chú ý là cả hai mô hình 5G đều đòi hỏi một không gian địa chỉ IP rất lớn, linh hoạt và hiệu quả – điều mà giao thức IPv6 hoàn toàn đáp ứng được. Chính vì vậy, sự phát triển của 5G không chỉ thúc đẩy nhu cầu chuyển đổi sang IPv6, mà còn cho thấy IPv6 là nền tảng tất yếu cho hệ sinh thái mạng thông minh trong tương lai.

IPv6 và 5G SA: Nền tảng cho tương lai

Sự kết hợp giữa IPv6 và 5G SA đang định hình nền tảng cho mạng di động hiện đại, được củng cố bởi các tiêu chuẩn từ 3GPP (Third Generation Partnership Project) và IETF (Internet Engineering Task Force). Theo tài liệu TS 23.501 của 3GPP, kiến trúc 5G SA tận dụng IPv6 để cung cấp địa chỉ duy nhất cho từng thiết bị, đảm bảo khả năng mở rộng cho hàng tỷ thiết bị, từ điện thoại thông minh đến hệ thống giao thông thông minh và IoT công nghiệp. Trong khi đó, IETF khuyến nghị triển khai mô hình "IPv6 Only" trên 5G để đơn giản hóa quản lý mạng và giảm chi phí vận hành. Một trong những tài liệu quan trọng như draft-ma-v6ops-5g-ipv6only-00 (tháng 02/2025) đề xuất sử dụng công nghệ 464XLAT nhằm duy trì dịch vụ IPv4 trên hạ tầng IPv6, hỗ trợ quá trình chuyển đổi thông suốt giữa hai giao thức.

Ứng dụng thực tế và xu hướng toàn cầu

Nhiều nhà mạng hàng đầu đã tiên phong triển khai 5G SA với IPv6:

China Telecom (Trung Quốc)

Ứng dụng 464XLAT để tối ưu hóa mạng 5G SA, hỗ trợ hàng triệu thiết bị IoT và cải thiện hiệu quả sử dụng tài nguyên mạng.

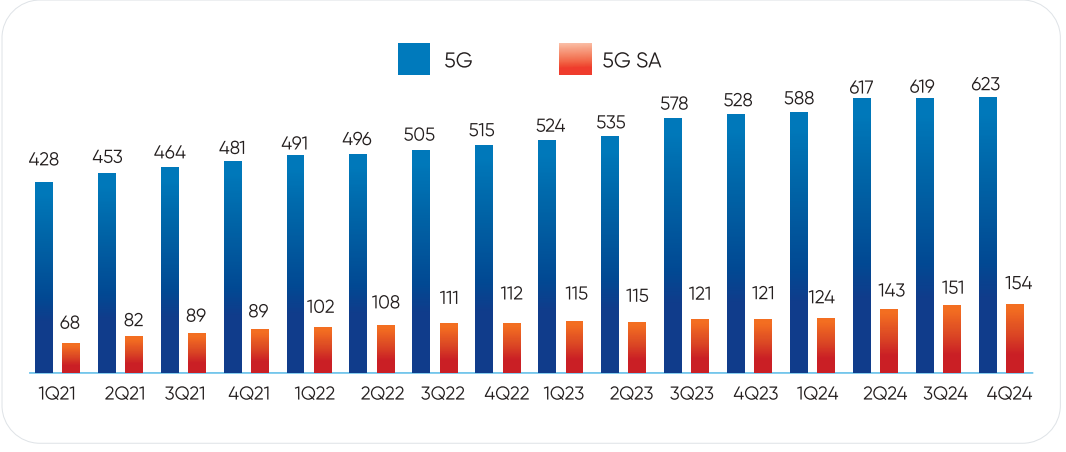
T-Mobile (Mỹ)

Tận dụng IPv6 để tăng tốc độ kết nối, giảm độ trễ và mở rộng hỗ trợ cho các ứng dụng IoT như nhà thông minh và giao thông thông minh.

Các nhà mạng châu Âu

Các công ty như Vodafone và Deutsche Telekom cũng đang chuyển đổi sang 5G SA với IPv6 để chuẩn bị cho các dịch vụ tương lai như y tế từ xa và thực tế tăng cường/ thực tế ảo (AR/VR).

Đến cuối năm 2024, trong 623 mạng 5G được triển khai trên thế giới thì đã có đến 154 mạng 5G độc lập, tương đương tỉ lệ 24,7% và số quốc gia triển khai 5G cũng đã lên đến con số 63. Như vậy mạng 5G độc lập và thuần IPv6 sẽ là xu hướng tất yếu trong tương lai, xu hướng này mở ra một kỷ nguyên mới, tạo ra những cơ hội mới và đáp ứng được những nhu cầu tiên tiến và đột phá hơn. Điều này đồng nghĩa tốc độ chuyển đổi sang IPv6 sẽ càng diễn ra mạnh mẽ với sự phát triển của mạng 5G và cả 6G trong tương lai.



Hình 12. Số liệu mạng 5G và 5G SA (nguồn: GSMA)

Lợi ích và tầm nhìn dài hạn

Sự hội tụ của IPv6 và 5G SA mang lại những lợi ích vượt trội sau:

Tốc độ và độ trễ

Tối ưu hóa việc truyền dữ liệu với độ trễ thấp, phù hợp cho các ứng dụng thời gian thực như phẫu thuật từ xa hoặc lái xe tự động.

Khả năng mở rộng

Hỗ trợ mật độ kết nối cao, lý tưởng cho các đô thị thông minh với hàng triệu cảm biến và thiết bị.

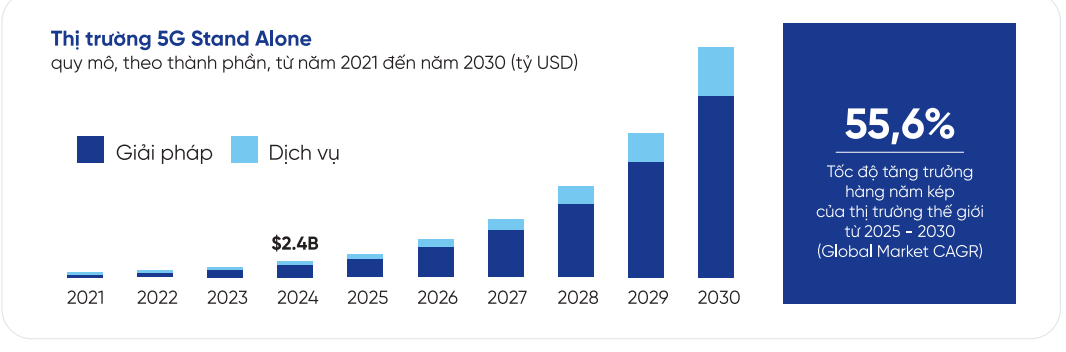
Bảo mật nâng cao

Kết nối toàn tuyến và mã hóa mạnh mẽ giúp bảo vệ dữ liệu trong các kịch bản nhạy cảm.

Hiệu quả kinh tế

Giảm phụ thuộc vào NAT và các giải pháp phức tạp, từ đó hạ thấp chi phí triển khai và vận hành dài hạn.

Nhìn xa hơn, sự kết hợp này không chỉ đáp ứng nhu cầu hiện tại mà còn đặt nền móng cho các công nghệ tương lai như mạng 6G, trí tuệ nhân tạo phân tán và hệ sinh thái số toàn diện. Với 5G SA và IPv6, ngành Viễn thông đang tiến tới một kỷ nguyên mà mọi thiết bị đều được kết nối một cách thông minh, an toàn và hiệu quả.



Hình 13. Thị trường 5G Stand Alone dự kiến (nguồn: www.grandviewresearch.com)

1.10. VAI TRÒ CỦA IPv6 VỚI IoT

IPv6 và IoT đang định hình tương lai Internet, tạo ra hệ sinh thái kết nối rộng lớn, bảo mật và linh hoạt. Với không gian địa chỉ khổng lồ, IPv6 chính là nền tảng lý tưởng cho sự bùng nổ của IoT. Tuy nhiên, thách thức lớn nhất không chỉ là số lượng thiết bị mà còn là sự phân mảnh công nghệ. IoT hiện sử dụng nhiều giao thức khác nhau như MQTT, CoAP, Websockets cùng hàng loạt chuẩn kết nối vô tuyến như Wi-Fi, Zigbee, LoRaWAN, SigFox, NB-IoT... IPv6 được kỳ vọng sẽ đóng vai trò là cầu nối, giúp hội tụ các công nghệ IoT, tạo ra một hệ sinh thái mở và thống nhất hơn.

Dự báo sự bùng nổ của IoT và vai trò của IPv6

IoT được dự đoán sẽ phát triển vượt bậc, với hơn 75 tỷ thiết bị kết nối toàn cầu vào năm 2030 theo Statista. Điều này đặt ra những thách thức chưa từng có về khả năng mở rộng địa chỉ, bảo mật và khả năng liên thông giữa các hệ thống IoT khác nhau. IPv6 được xem là công nghệ cốt lõi giúp giải quyết những vấn đề này, nhờ vào không gian địa chỉ gần như vô hạn, khả năng hỗ trợ kết nối đầu cuối (End-to-End) và các tính năng bảo mật tích hợp như IPsec, Extension Headers và Secure Neighbor Discovery (SEND).

Thách thức lớn nhất của IoT: Sự phân mảnh công nghệ

Vấn đề của IoT không chỉ nằm ở số lượng thiết bị khổng lồ, mà còn nằm ở sự đa dạng của các công nghệ và giao thức kết nối. Hiện nay, hệ sinh thái IoT đang sử dụng nhiều công nghệ, giao thức mạng khác nhau, có đặc điểm riêng về băng thông, độ trễ, mức tiêu thụ năng lượng và phạm vi kết nối, dẫn đến sự thiếu thống nhất và khó khăn trong việc mở rộng quy mô hệ sinh thái IoT, ví dụ như:

Giao thức ứng dụng:
MQTT, CoAP, Websockets, AMQP, DDS, OPC UA...

Chuẩn liên kết dữ liệu và kết nối vô tuyến:
Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRa, SigFox, NB-IoT, LTE-M, DASH7, IEEE 802.15.4...

Hình 14. Các công nghệ được sử dụng trong IoT

IPv6: Nền tảng hội tụ và mở rộng IoT

Trong các giai đoạn phát triển của mạng viễn thông – từ 2.5G đến 5G – giao thức IPv4 từng đóng vai trò quan trọng trong việc triển khai nhiều dịch vụ như VoIP, IPTV hay hệ thống giám sát IP Camera. Tuy nhiên, với sự phát triển nhanh chóng và phân mảnh của Internet vạn vật (IoT), mô hình kết nối dựa trên IPv4 ngày càng bộc lộ rõ những hạn chế về không gian địa chỉ, khả năng định danh, cũng như mức độ bảo mật và mở rộng.

Trong bối cảnh đó, IPv6 được xem là công nghệ chiến lược giúp hội tụ và thống nhất hệ sinh thái IoT toàn cầu. Với không gian địa chỉ gần như vô hạn, hỗ trợ tự động cấu hình, bảo mật tích hợp (IPsec) và khả năng hoạt động hiệu quả trên quy mô lớn, IPv6 chính là chìa khóa để hiện thực hóa một thế giới "mọi thứ đều được kết nối".

Sự kết hợp giữa IoT và IPv6, được hỗ trợ bởi mạng 5G/6G và các tiêu chuẩn của tổ chức 3GPP, sẽ mở đường cho các ứng dụng tiên tiến như y tế từ xa, giao thông tự hành, nông nghiệp thông minh, nhà máy số và thành phố thông minh. Nhờ IPv6, mỗi thiết bị IoT – từ cảm biến đến rô bốt công nghiệp – đều có thể được kết nối, định danh và quản lý một cách hiệu quả và bảo mật.

Hơn thế nữa, tương lai của IoT và IPv6 sẽ ngày càng gắn kết chặt chẽ với sự phát triển của AIoT (AI + IoT) và điện toán biên (Edge Computing). Sự hội tụ này sẽ hình thành nên một hệ sinh thái kết nối thông minh, hiệu quả và an toàn hơn, cho phép xử lý dữ liệu tại nguồn, giảm độ trễ và tối ưu hóa hiệu suất hoạt động trên toàn mạng lưới.

Như vậy, IPv6 không còn là một lựa chọn, mà là yếu tố tất yếu để xây dựng hạ tầng IoT hiện đại, bền vững, mở rộng và bảo mật trong kỷ nguyên số. Việc chuyển đổi sang IPv6 chính là điều kiện tiên quyết để các quốc gia, doanh nghiệp và tổ chức bắt kịp xu thế phát triển của cách mạng công nghiệp 4.0 và Internet of Everything (IoE).

IETF và các tiêu chuẩn IPv6 cho IoT

Nhằm tối ưu IPv6 cho IoT, IETF đã phát triển nhiều tiêu chuẩn, trong đó quan trọng nhất là:

1. 6LoWPAN (RFC 6282)

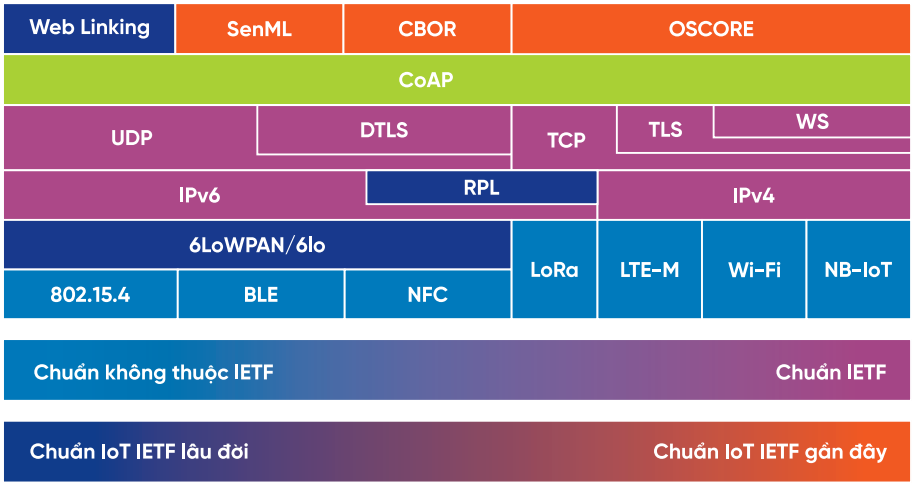
Chuẩn IPv6 đầu tiên cho IoT, được thiết kế để hoạt động trên nền tảng IEEE 802.15.4 (mạng cảm biến công suất thấp). 6LoWPAN hỗ trợ nén Header IPv6, giúp giảm kích thước gói tin, tiết kiệm băng thông và tối ưu năng lượng.

2. 6Lo (IPv6 over constrained nodes)

Mở rộng 6LoWPAN để hỗ trợ nhiều loại mạng vật lý khác như Bluetooth Low Energy (BLE), DECT-ULE, NFC, PLC...

3. LPWAN over IPv6

Một số giao thức LPWAN (Low Power Wide Area Network) như LoRaWAN, SigFox đang triển khai IPv6 để tăng khả năng liên thông và bảo mật.



Hình 15. Các chuẩn giao thức IoT liên quan đến IPv6

1.11. NHỮNG LỢI ÍCH IPv6 MANG LẠI

Sự ra đời của IPv6 xuất phát chính từ sự cạn kiệt của giao thức IPv4, tại thời điểm ban đầu có hai đề xuất thiết kế cho giao thức mới này:

- Giữ nguyên đặc điểm của giao thức IPv4 và mở rộng số bit cho phần địa chỉ (ví dụ lên 64 bit).
- Xây dựng một giao thức mới dựa trên nền tảng giao thức IPv4 nhưng tối ưu những điểm hạn chế và phát triển tính năng mới.

Sau các cuộc thảo luận, cuối cùng giải pháp thứ hai, xây dựng giao thức mới, đã được thống nhất. Nhiều tính năng cũ của IPv4 đã được loại bỏ hoặc thay thế, đồng thời nhiều giao thức hỗ trợ mới được bổ sung. Việc này đã giúp giao thức IPv6 mang lại rất nhiều ưu điểm so với IPv4.

Dưới đây là những lợi ích quan trọng nhất của giao thức IPv6:

Không gian địa chỉ gần như vô hạn:

Số bit địa chỉ IPv6 là 128 bit, tăng gấp bốn lần so với IPv4, nên đáp ứng tốt nhu cầu phát triển của mạng Internet cũng như yêu cầu của các công nghệ mới như: IoT, 5G-6G, điện toán đám mây ...

Cấu trúc gói tin đơn giản hơn:

Việc này giúp tăng tốc độ xử lý các gói tin. Bên cạnh đó, sự bổ sung thêm thành phần mở rộng như Extension Header, Flow ... giúp triển khai thêm nhiều tính năng tiên tiến.

Cho phép kết nối toàn tuyến (End-to-End):

Giúp giải quyết vấn đề do NAT/PAT gây ra và loại bỏ các giải pháp "chữa cháy" khác CG-NAT, CIDR, VLSM ...

Đơn giản hóa việc quản trị, khai thác:

Một số cải thiện liên quan IPv6 giúp đơn giản hóa khai báo và hoạt động của thiết bị như tự cấu hình địa chỉ (SLAAC), loại bỏ Broadcast, bỏ ARP, IGMP, cải thiện ICMPv6 ...

Tối ưu về định tuyến:

Do số lượng địa chỉ IPv6 lớn nên các đơn vị sẽ được cấp dãy lớn hơn (thường /48), đáp ứng nhu cầu phát triển lâu dài của các đơn vị, ít cần phải đăng ký thêm nên bảng định tuyến toàn cầu sẽ gọn hơn, giúp tăng tốc độ xử lý cũng như tiết kiệm bộ nhớ cho các các thiết bị định tuyến.

Hỗ trợ Multicast tốt hơn:

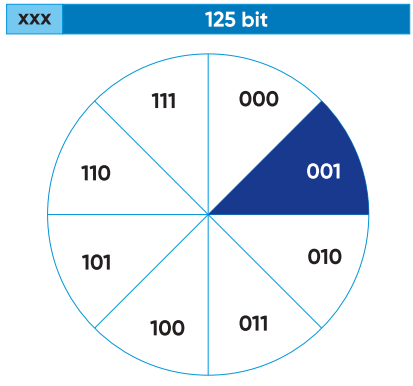
Tính năng Multicast trong IPv6 được cải tiến, giúp loại bỏ địa chỉ Broadcast, địa chỉ Solicited Multicast giúp loại bỏ các hoạt động dựa trên cơ chế Broadcast như ARP, giúp kiểm trùng địa chỉ, giúp thiết bị tự cấu hình địa chỉ và Gateway ...

Cải thiện bảo mật:

Kỹ thuật bảo mật của IPSec đã được tích hợp thành tính năng của IPv6 cùng với việc loại bỏ kỹ thuật NAT giúp cho việc trao đổi dữ liệu giữa hai thiết bị được bảo mật toàn tuyến.

1.12. PHÂN VÙNG KHÔNG GIAN ĐỊA CHỈ IPv6

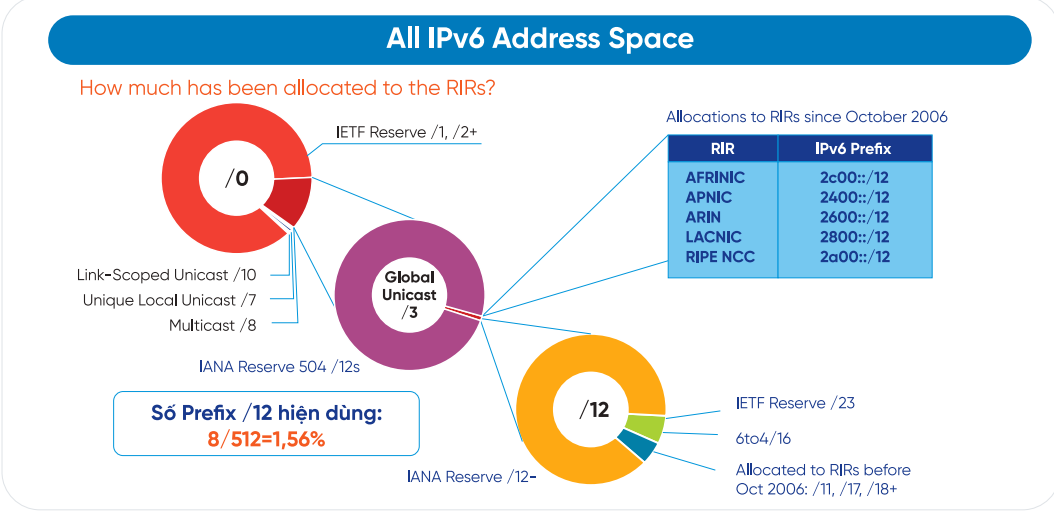
Để quản lý và phân bổ địa chỉ IPv6 hiệu quả, IANA đã chia toàn bộ không gian địa chỉ IPv6 thành tám phân vùng bằng nhau, dựa trên ba bit đầu tiên của địa chỉ. Mỗi phân vùng này có địa chỉ mạng đại diện là /3.



Hình 16. Các vùng địa chỉ IPv6

Hiện tại, phân vùng có tiền tố "001" (/3) được sử dụng để cấp phát địa chỉ IPv6 công khai (tương tự như địa chỉ Public IPv4) và được gọi là Global Unicast Address. Ngoài ra, một số phân vùng khác với tiền tố "000" và "111" được sử dụng cho các địa chỉ đặc biệt như Multicast, Unique Local Unicast, Loopback...

IANA tiếp tục chia nhỏ phân vùng "001" (/3) thành các dãy /12 trước khi phân bổ cho các tổ chức quản lý khu vực (RIR). Tổng số dãy /12 trong phân vùng này là: **2^9 = 512 dãy /12.**

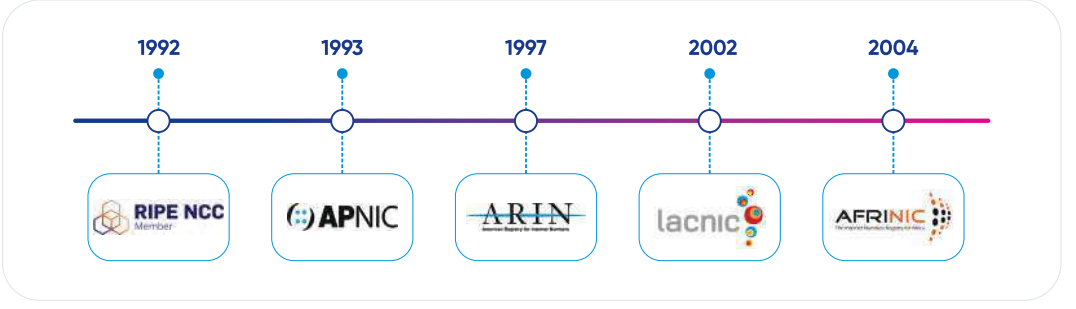


Hình 17. Số lượng dãy địa chỉ IPv6 phân bổ cho RIR (nguồn: NRO)

Ban đầu IANA chỉ dùng một dãy /12 để phân bổ cho các khu vực và cấp phát cho các mục đích khác. Sau này, trước nhu cầu phát triển của IPv6, từ năm 2006 IANA đã bắt đầu phân bổ các dãy /12 cho các RIR. Đến nay đã có tất cả 8 dãy /12 đã được cấp phát thực tế trên toàn cầu, chiếm tỉ lệ: 8/512=1,56%. Như vậy, từ năm 2006 đến nay, chỉ chưa đến 2% của 1/8 tổng không gian địa chỉ IPv6 được phân bổ và các tổ chức khu vực vẫn chưa sử dụng hết số lượng được cấp. Điều này cho thấy không gian địa chỉ IPv6 vẫn còn rất lớn, đủ để đáp ứng nhu cầu phát triển mạng Internet trong tương lai.

1.13. CƠ QUAN QUẢN LÝ VÀ CẤP PHÁT ĐỊA CHỈ IP

Trên mạng Internet, mỗi địa chỉ IP là duy nhất nên có sự quản lý cấp phát địa chỉ IP thống nhất trên toàn cầu. Đồng thời trước sự phát triển của mạng Internet, nhu cầu cấp phát địa chỉ toàn cầu tăng lên rất cao. Năm 1992, IETF khuyến cáo việc quản lý địa chỉ IP cần chuyển giao cho các tổ chức cấp khu vực trên thế giới. Từ đó các tổ chức quản lý tài nguyên cấp khu vực RIR (Regional Internet Registry) lần lượt được thành lập, gồm năm (05) tổ chức nằm ở các khu vực địa lý khác nhau.



Hình 18. Tên 5 tổ chức quản lý vùng và thời gian thành lập

RIPE NCC (Réseaux IP Européens Network Coordination Centre): được thành lập năm 1992 để quản lý phân bổ tài nguyên Internet cho khu vực châu Âu và Trung Đông.

APNIC (Asia-Pacific Network Information Centre): được thành lập năm 1993, chịu trách nhiệm quản lý khu vực châu Á và một số quốc gia, lãnh thổ thuộc khu vực Thái Bình Dương.

ARIN (American Registry for Internet Numbers): được thành lập năm 1997, phạm vi quản lý là khu vực Bắc Mỹ, một số quốc gia thuộc Trung Mỹ và vùng Caribbean.

LACNIC (Latin American and Caribbean Internet Addresses Registry) - thành lập năm 2002 để quản lý phân chia địa chỉ IP ở khu vực Mỹ Latinh và Caribe.

AfriNIC (African Network Information Centre): được công nhận thành lập từ năm 2004 và bắt đầu hoạt động chính thức năm 2005 với phạm vi quản lý ở khu vực châu Phi.

Hình 19. Phạm vi quản lý của 5 tổ chức cấp vùng

Mỗi RIR sẽ chịu trách nhiệm quản lý và phân bổ địa chỉ IP (và cả số hiệu mạng Internet ASN - Autonomous System Number) cho các quốc gia trong khu vực. Tại mỗi quốc gia sẽ có một đơn vị chịu trách nhiệm phân bổ và quản lý địa chỉ IP/ASN được gọi là NIR (National Internet Registry) hoặc LIR (Local Internet Registry). Các RIR phân bổ tài nguyên này cho NIR (National Internet Registry) hoặc trực tiếp cho LIR (Local Internet Registry).

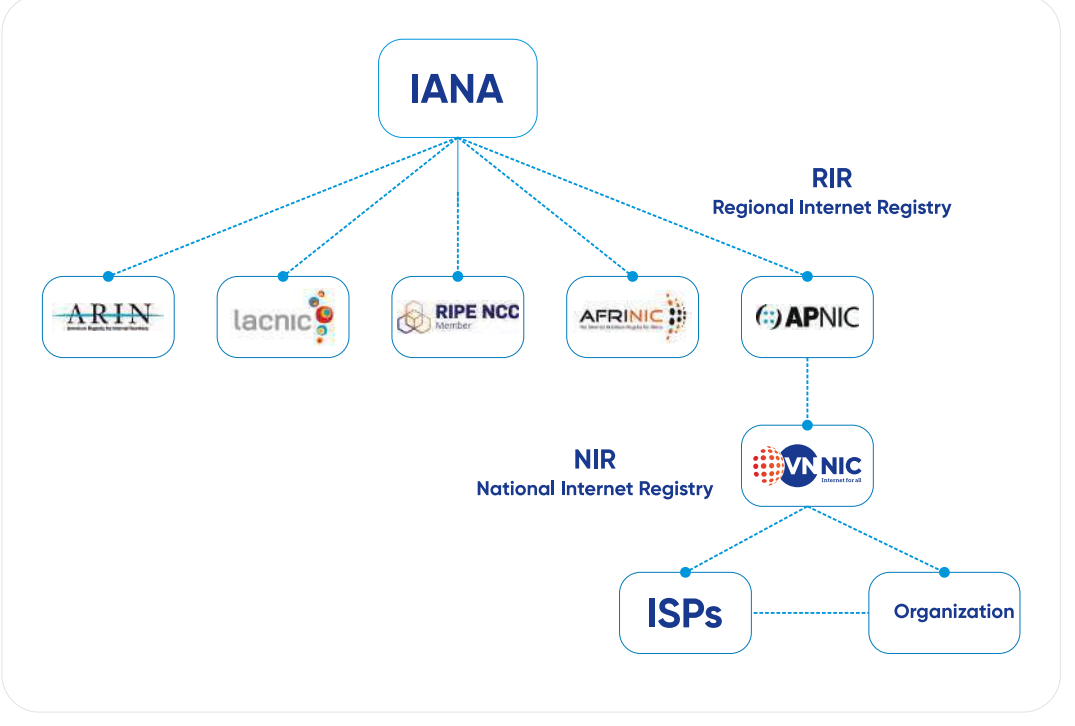
Tại Việt Nam, Trung tâm Internet Việt Nam (VNNIC) đóng vai trò là NIR, chịu trách nhiệm cấp phát và quản lý địa chỉ IP cũng như ASN trong nước. VNNIC cấp địa chỉ trực tiếp cho các nhà mạng (ISP), doanh nghiệp lớn và tổ chức có nhu cầu sử dụng tài nguyên IP độc lập. Có hai hình thức sử dụng địa chỉ IP:

PI (Provider Independent)

Địa chỉ độc lập, do VNNIC cấp trực tiếp cho tổ chức/doanh nghiệp, có thể sử dụng mà không phụ thuộc vào một nhà cung cấp dịch vụ nào.

PA (Provider Aggregatable)

Địa chỉ phụ thuộc, được các ISP cấp cho khách hàng, thường phải trả phí định kỳ cho ISP và trả lại địa chỉ khi thay đổi nhà cung cấp dịch vụ.



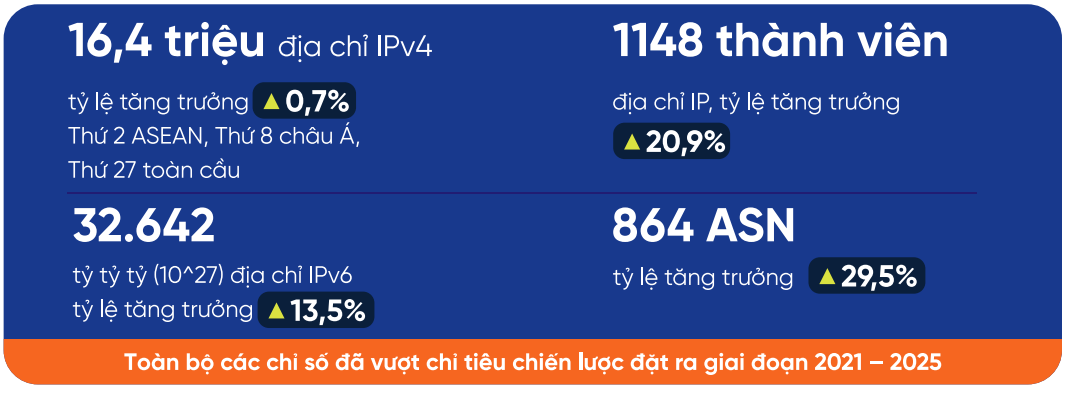
Hình 20. Mối liên hệ giữa IANA, các RIR & NIR

1.14 GIỚI THIỆU VỀ TRUNG TÂM INTERNET VIỆT NAM (VNNIC)

Trung tâm Internet Việt Nam (VNNIC), trực thuộc Bộ Khoa học và Công nghệ (trước đây là đơn vị thuộc Bộ Thông tin và Truyền thông), là cơ quan chịu trách nhiệm quản lý toàn diện tài nguyên Internet tại Việt Nam. Với vai trò này, VNNIC thực hiện phân bổ và giám sát các tài nguyên quan trọng như địa chỉ IP (IPv4 và IPv6), số hiệu mạng ASN (Autonomous System Number) và tên miền quốc gia ".vn".

Bên cạnh đó, VNNIC cũng trực tiếp vận hành hai hệ thống hạ tầng cốt lõi của Internet Việt Nam: Hệ thống máy chủ tên miền quốc gia (DNS .vn) và Trạm trung chuyển Internet quốc gia (VNIX – Vietnam National Internet Exchange).

Không chỉ đóng vai trò quản lý, VNNIC còn tích cực phát triển tên miền ".vn", góp phần xây dựng và bảo vệ thương hiệu quốc gia trên không gian số. Hệ thống DNS và VNIX giúp tối ưu hóa kết nối nội địa, giảm độ trễ, nâng cao chất lượng dịch vụ và tăng cường bảo mật cho các nền tảng trực tuyến, mang lại trải nghiệm mạng nhanh chóng, ổn định và tin cậy cho người dùng và doanh nghiệp trong nước.



Hình 21. Số liệu về địa chỉ IP/ASN Việt Nam (nguồn: Báo cáo tài nguyên Internet năm 2024 của VNNIC)

Với vai trò là đơn vị tiên phong trong chuyển đổi sang IPv6, VNNIC đã đề xuất và thực hiện nhiều chính sách, chiến lược và chương trình đào tạo, hỗ trợ kỹ thuật cho các cơ quan, doanh nghiệp và tổ chức. Việc chuyển đổi từ IPv4 sang IPv6 không chỉ giúp giải quyết tình trạng cạn kiệt địa chỉ, mà còn đặt nền móng cho một hạ tầng mạng hiện đại, sẵn sàng đáp ứng các xu hướng công nghệ mới như IoT, 5G, AIoT và các dịch vụ số thông minh. Nhờ những nỗ lực này, Việt Nam đã vươn lên nhóm các quốc gia dẫn đầu khu vực và toàn cầu về tỷ lệ triển khai và ứng dụng IPv6.

Ngoài ra, VNNIC còn đóng vai trò là cầu nối giữa cộng đồng Internet Việt Nam và quốc tế. Thông qua hợp tác với các tổ chức như APNIC và các diễn đàn khu vực, VNNIC giúp các doanh nghiệp trong nước tiếp cận chuẩn mực toàn cầu, đồng thời đảm bảo hạ tầng Internet quốc gia phát triển bền vững, an toàn, có khả năng mở rộng và đáp ứng nhu cầu của xã hội số. Nhờ những đóng góp này, VNNIC đã khẳng định vị thế không thể thay thế trong việc kiến tạo hệ sinh thái Internet Việt Nam, đồng thời nâng cao sự hiện diện của Việt Nam trên bản đồ Internet toàn cầu.

1.15 TỔNG KẾT CHƯƠNG 1

IPv6 – Hành trình tất yếu của một Internet hiện đại. Chương này đã trình bày tổng quan các nội dung nền tảng về sự ra đời và phát triển của giao thức IPv6 – từ dự báo sớm về nguy cơ cạn kiệt địa chỉ IPv4, đến quá trình nghiên cứu và đề xuất giao thức mới của IETF, cùng với các sự kiện thúc đẩy thực tiễn như World IPv6 Day và World IPv6 Launch do ISOC tổ chức.

Sự kết hợp giữa sự phát triển công nghệ, yêu cầu hạ tầng mạng hiện đại và những nỗ lực toàn cầu trong việc triển khai IPv6 đã cho thấy giao thức này đã chín muồi, sẵn sàng thay thế IPv4 để đáp ứng các nhu cầu kết nối mới. Từ IoT, 5G, đến AI, điện toán biên và dịch vụ số thông minh, IPv6 chính là nền tảng tất yếu để xây dựng một mạng Internet thế hệ mới, thông minh, an toàn và không giới hạn.

1.16 CÂU HỎI ÔN TẬP CHƯƠNG 1

01 Tại sao giao thức IPv4 cần được thay thế bằng IPv6?

Giao thức IPv4, mặc dù rất thành công và là nền tảng của Internet, đã bộc lộ những hạn chế, đặc biệt là sự cạn kiệt không gian địa chỉ 32 bit. Sự phát triển bùng nổ của Internet và số lượng thiết bị kết nối ngày càng tăng đã dẫn đến nhu cầu cấp thiết về một không gian địa chỉ lớn hơn, đó là lý do chính cho sự ra đời của IPv6.

02 Quá trình phát triển từ IPv4 đến IPv6 diễn ra như thế nào?

Ý tưởng về thế hệ IP tiếp theo đã xuất hiện từ đầu những năm 1990 khi các chuyên gia nhận thấy nguy cơ cạn kiệt địa chỉ IPv4. Tổ chức IETF đã kêu gọi các đề xuất và sau nhiều tranh luận và lựa chọn giữa các phương án như TUBA, CATNIP, SIPP, cuối cùng giao thức SIPP với địa chỉ 128 bit đã được chọn và đổi tên thành IPv6, chính thức được giới thiệu trong RFC 1883 vào năm 1995.

03 Những lợi ích chính mà IPv6 mang lại so với IPv4 là gì?

IPv6 mang lại nhiều lợi ích vượt trội so với IPv4, bao gồm không gian địa chỉ gần như vô hạn (128 bit), cấu trúc gói tin đơn giản hơn giúp tăng tốc độ xử lý, khả năng kết nối toàn tuyến (End-to-End) loại bỏ nhu cầu NAT, đơn giản hóa quản trị và khai thác mạng với khả năng tự cấu hình địa chỉ, tối ưu hóa định tuyến, hỗ trợ multicast tốt hơn và tích hợp sẵn bảo mật IPSec.

04 Các tổ chức nào đóng vai trò quản lý và cấp phát địa chỉ IP trên toàn cầu và tại Việt Nam?

Tổ chức IANA (Internet Assigned Numbers Authority) chịu trách nhiệm quản lý và phân bổ địa chỉ IP toàn cầu. IANA phân chia địa chỉ cho năm tổ chức quản lý tài nguyên cấp vùng RIR (Regional Internet Registry) là RIPE NCC, APNIC, ARIN, LACNIC và AfriNIC. Tại Việt Nam, Trung tâm Internet Việt Nam (VNNIC) đóng vai trò là NIR (National Internet Registry), chịu trách nhiệm quản lý, phân bổ, cấp địa chỉ IP địa chỉ IP, số hiệu mạng ASN và tên miền quốc gia ".vn".

05 Tình hình triển khai và chuyển đổi sang IPv6 trên thế giới và tại Việt Nam hiện nay (2025) như thế nào?

Trên toàn cầu, tỷ lệ người dùng IPv6 đã tăng trưởng đáng kể, đạt gần 48% vào đầu tháng 3/2025. Việt Nam là một trong những quốc gia tiên phong trong việc chuyển đổi IPv6, với tỷ lệ người dùng đạt 65,5% vào cuối năm 2024, nằm trong Top 10 thế giới và thứ 2 trong khu vực ASEAN. Việt Nam cũng đang có lộ trình hướng tới việc chuyển đổi hoàn toàn sang IPv6 Only.

06 Mối liên hệ giữa IPv6 và các công nghệ hiện đại như 5G và IoT là gì?

IPv6 đóng vai trò nền tảng quan trọng cho sự phát triển của 5G và IoT. Với số lượng địa chỉ khổng lồ, IPv6 đáp ứng tốt nhu cầu kết nối số lượng lớn thiết bị của 5G và IoT. Cấu trúc gói tin đơn giản và khả năng kết nối End-to-End của IPv6 cũng giúp giảm độ trễ và tăng cường bảo mật cho các ứng dụng 5G. Trong lĩnh vực IoT, các chuẩn như 6LoWPAN đang được phát triển để tối ưu hóa việc truyền tải dữ liệu IPv6 trên các thiết bị có tài nguyên hạn chế.

07 Tại sao các kỹ thuật tiết kiệm địa chỉ IPv4 như NAT, CIDR, VLSM không còn cần thiết trong môi trường IPv6?

Với không gian địa chỉ 128 bit, IPv6 cung cấp một số lượng địa chỉ gần như vô hạn. Điều này làm cho các kỹ thuật tiết kiệm địa chỉ IPv4 như NAT (Network Address Translator), CIDR (Classless Inter-Domain Routing) và VLSM (Variable Length Subnet Mask) trở nên không cần thiết, vì mỗi thiết bị có thể được gán một địa chỉ IPv6 duy nhất và công khai.

08 Việt Nam có kế hoạch gì cho tương lai liên quan đến việc sử dụng IPv4 và IPv6?

Việt Nam đã có những chiến lược và hành động quyết liệt để thúc đẩy chuyển đổi sang IPv6. Với tỷ lệ triển khai IPv6 cao, Việt Nam đang hướng tới mục tiêu chuyển đổi toàn bộ mạng Internet sang hoạt động với IPv6 theo Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030; Quy hoạch ngành Thông tin và Truyền thông thời kỳ 2021 - 2030, tầm nhìn đến năm 2050. VNNIC đã đề xuất Lộ trình chuyển đổi Internet Việt Nam sang IPv6 only; tổ chức thí điểm IPv6 only từ năm 2025, nhân rộng trong giai đoạn 2026 - 2030; mục tiêu ngừng sử dụng IPv4 và sử dụng hoàn toàn IPv6 only vào năm 2032.

PHẦN 1 – LÝ THUYẾT

CHƯƠNG 2

CẤU TRÚC & ĐẶC ĐIỂM GIAO THỨC IPv6

CHƯƠNG 2

CẤU TRÚC & ĐẶC ĐIỂM GIAO THỨC IPv6

Vấn đề cạn kiệt địa chỉ IPv4 là một trong những nguyên nhân chính thúc đẩy sự ra đời của IPv6, nhưng đó chỉ là một khía cạnh. Trong thực tiễn triển khai, chính kiến trúc hiện đại và các tính năng kỹ thuật vượt trội mới là yếu tố then chốt thuyết phục các cơ quan, tổ chức và doanh nghiệp trên toàn thế giới lựa chọn IPv6 như một giải pháp lâu dài, thay thế hoàn toàn cho IPv4.

Chương 2 sẽ tập trung vào cấu trúc và các đặc điểm kỹ thuật của giao thức IPv6, đồng thời so sánh nó với IPv4 để làm nổi bật những cải tiến. Nội dung sẽ cho thấy kiến trúc và các tính năng mới của IPv6 là yếu tố then chốt thúc đẩy việc chuyển đổi từ IPv4. Đặc biệt, chương này đi sâu vào cấu trúc bản tin IPv6, nhấn mạnh vai trò của tiêu đề chính cố định và sự linh hoạt của tiêu đề mở rộng (Extension Headers), một cơ chế cho phép thêm các chức năng tùy chọn mà không làm thay đổi cấu trúc cơ bản của giao thức.

CỤ THỂ, CHƯƠNG 2 SẼ CUNG CẤP CHO BẠN NHỮNG NỘI DUNG SAU:

Kiến trúc và đặc điểm kỹ thuật của giao thức IPv6, bao gồm sự so sánh với IPv4 để dễ dàng nắm bắt.

Cấu trúc bản tin của giao thức IPv6, đi sâu vào chức năng và vai trò của từng trường, đặc biệt là tiêu đề mở rộng (Extension Headers).

Mối quan hệ giữa IPv4, IPv6 và bộ giao thức TCP/IP, cả hai có thể hoạt động song song mà không làm thay đổi kiến trúc chung của TCP/IP.

Sự thay thế và cập nhật của các giao thức hỗ trợ khi chuyển từ IPv4 sang IPv6, ví dụ như ARP thay bằng NDP, IGMP thay bằng MLD và việc giữ lại, cập nhật của ICMP.

Vai trò và cấu trúc của tiêu đề mở rộng (Extension Header), giới thiệu một số tiêu đề mở rộng phổ biến và mục đích sử dụng của chúng.

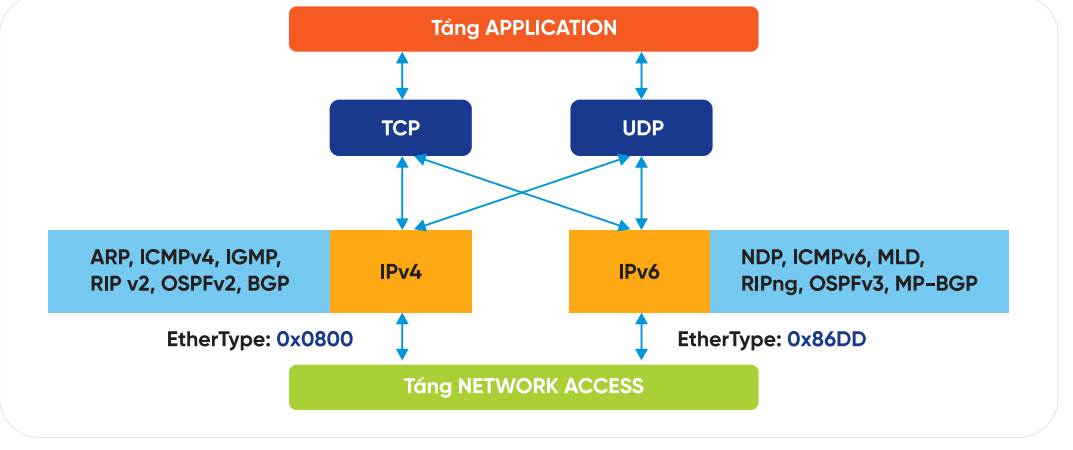
2.1 IPv4, IPv6 VÀ BỘ GIAO THỨC TCP/IP

TCP/IP không phải là một giao thức đơn lẻ, mà là một bộ tập hợp nhiều giao thức được tổ chức thành các lớp chức năng, ánh xạ tương ứng với mô hình 7 lớp OSI. Trong đó, IP (Internet Protocol) là giao thức thuộc tầng mạng, chịu trách nhiệm định tuyến và truyền tải dữ liệu giữa các hệ thống mạng khác nhau. Tuy nhiên, IP không hoạt động độc lập mà cần sự hỗ trợ của nhiều giao thức cùng tầng mạng, đặc biệt trong trường hợp của IPv4. Một số giao thức hỗ trợ quan trọng gồm:

- ICMPv4, (thông báo lỗi, chẩn đoán)
- ARP, (phân giải địa chỉ IP sang MAC)
- IGMP (quản lý nhóm multicast)
- OSPFv2, RIPv2, BGPv4, IGMP, ...(định tuyến)

Tất cả những giao thức này đều trên hoạt động dựa trên nền IPv4, phục vụ cho việc quản lý, định tuyến và duy trì kết nối trong mạng.

Khi IPv6 ra đời để thay thế IPv4, nó được đặt cùng tầng mạng trong mô hình TCP/IP và không làm thay đổi kiến trúc tổng thể của bộ giao thức. Điều quan trọng là IPv6 vẫn đảm bảo khả năng tương thích với các tầng giao thức khác như TCP, UDP, ứng dụng – các tầng này không cần thay đổi để hoạt động với IPv6.



Hình 22. IPv4, IPv6 và các giao thức hỗ trợ

Tuy nhiên, do kiến trúc IPv6 có nhiều khác biệt với IPv4, nên nhiều giao thức hỗ trợ tầng mạng đã được thay thế hoặc cập nhật:

Giao thức trong IPv4	Tương đương / thay thế trong IPv6
ARP (Address Resolution)	NDP (Neighbor Discovery Protocol)
IGMP (Multicast)	MLD (Multicast Listener Discovery)
ICMPv4	ICMPv6 (được mở rộng thêm chức năng)
OSPFv2	OSPFv3
RIP v2	RIPng (RIP next generation)

Sự chuyển đổi này không chỉ nhằm đảm bảo tương thích với IPv6, mà còn là cơ hội để cải tiến và loại bỏ các hạn chế từng tồn tại trong hệ thống IPv4. Ví dụ, NDP tích hợp nhiều chức năng mà ARP, ICMPv4 và một phần DHCP từng thực hiện riêng rẽ.

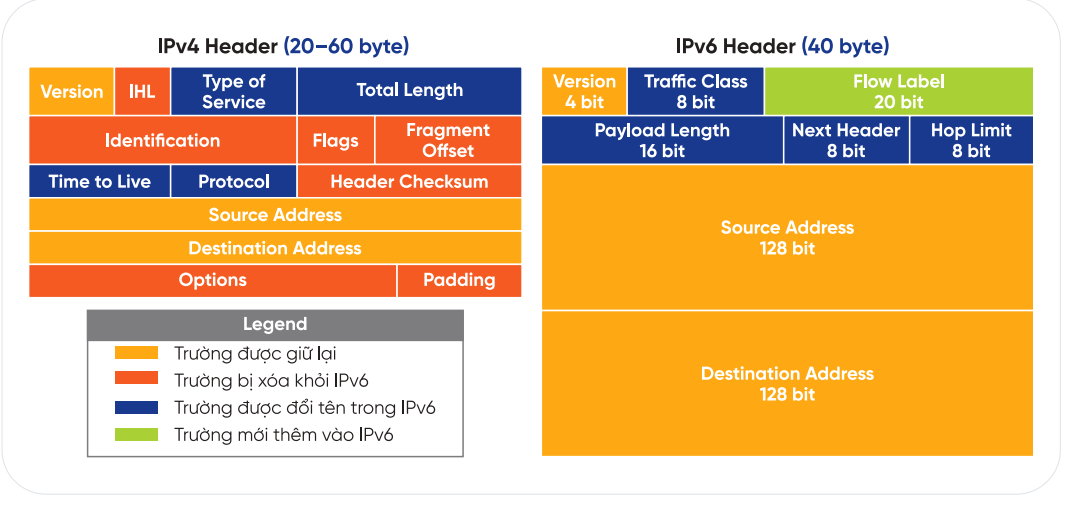
Một điểm lưu ý về khả năng nhận diện IPv6 ở tầng liên kết dữ liệu: trong môi trường Ethernet, bản tin IPv6 được phân biệt bằng EtherType 0x86DD, trong khi IPv4 sử dụng 0x0800. Điều này giúp các thiết bị mạng xác định và xử lý đúng loại gói tin IP.

Tóm lại, sự xuất hiện của IPv6 không làm thay đổi cấu trúc chung của bộ TCP/IP, nhưng **đòi hỏi điều chỉnh các giao thức hỗ trợ ở tầng mạng** để phù hợp với thiết kế mới, hiện đại và hiệu quả hơn. Đây chính là một trong những yếu tố kỹ thuật quan trọng góp phần vào thành công của IPv6 trong thực tế triển khai.

2.2 CẤU TRÚC BẢN TIN CỦA IPv6 VÀ NHỮNG CẢI TIẾN

Do IPv6 được thiết kế thay thế cho IPv4 nên có rất nhiều điểm tối ưu hơn dựa trên những kinh nghiệm rút ra từ IPv4. Để hiểu rõ đặc tính và hoạt động chi tiết của IPv6 thì cần phải hiểu trúc bản tin của IPv6. Cấu trúc này được mô tả trong RFC 2460. Sau đây là số điểm chính trong cấu trúc IPv6 so với IPv4 gồm:

- Kích thước tiêu đề bản tin (Header) IPv6 cố định 40 byte trong khi IPv4 thay đổi từ 20 đến 60 byte.
- Số trường trong phần Header của IPv6 ít hơn so với IPv4 nên gọn hơn.
- Một số trường chính của IPv4 được giữ lại nguyên tên hoặc đổi sang tên mới.
- Vài trường mới được bổ sung, đặc biệt là phần mở rộng Header Extension, giúp IPv6 hoạt động tối ưu hơn cũng như bổ sung thêm nhiều tính năng quan trọng.



Hình 23. So sánh IPv4 và IPv6 Header

Phần Header của IPv4 có đến 14 trường, trong khi IPv6 chỉ có 8 trường và cố định ở 40 byte nên giúp việc xử lý bản tin IPv6 nhanh hơn so với IPv4. Dưới đây là so sánh chi tiết của các trường của IPv4 so với IPv6 để các bạn hiểu rõ hơn cách thức hoạt động của giao thức IPv6.

Những trường được giữ lại và để nguyên tên:

Version

Trường này dài 4 bit để chỉ phiên bản của giao thức IP, không có khác biệt ở trường này, chỉ là giá trị 4 hoặc 6.

Source/Destination Adrress

Hai trường này cùng ý nghĩa ở hai giao thức chỉ có sự khác biệt là địa chỉ IPv6 có độ dài 128 bit, gấp 4 lần địa chỉ IPv4.

Những trường được giữ lại và đổi tên:

Type of Service

Đối với IPv6 trường 8 bit này vẫn được giữ lại với cùng chức năng nhằm phân loại ưu tiên các bản tin nhưng với tên mới là **Traffic Class.**

Total Length

Với IPv4 trường 16 bit này dùng để mô tả chiều dài (tính bằng byte) toàn bộ bản tin IPv4, với 16 bit thì kích thước bản tin lớn nhất của IPv4 là 65.536 byte. Sang IPv6 trường này vẫn được giữ lại có cùng kích thước 16 bit nhưng có tên mới là **Payload Length**. Do phần Header của IPv6 là cố định nên Payload Length chỉ mô tả kích thước phần dữ liệu Payload của bản tin IPv6 thay vì kích thước toàn bộ bản tin như IPv4.

Time to live

Trường 8 bit này giúp phòng chống việc truyền lặp (Loop) các bản tin bằng cách giảm giá trị bằng 1 tại mỗi Router cho đến khi bằng 0 thì bản tin bị loại bỏ. Với IPv6, trường này chỉ thay đổi sang tên mới là Hop Limit, chức năng và ý nghĩa không thay đổi.

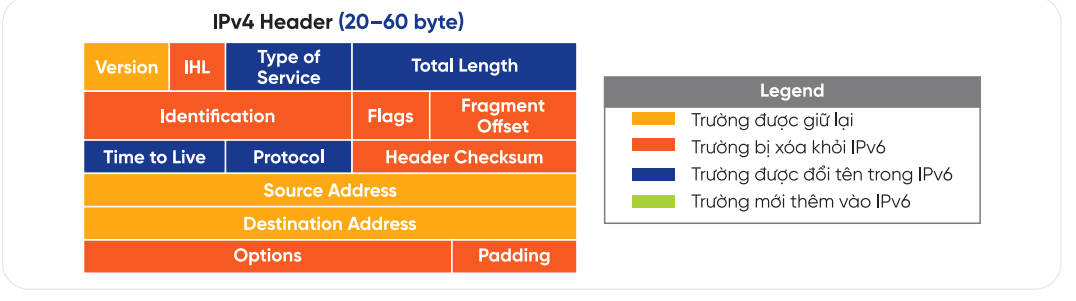
Protocol

Với IPv4, trường này chứa thông tin giao thức nằm trong phần Payload của bản tin IPv4. Sang IPv6 trường này vẫn được giữ lại và đổi tên thành Next Header. Nhưng thiết kế mới của IPv6 cho phép chèn một số thông tin vào giữa phần Header và Payload ban đầu để thực hiện một số chức năng nào đó. Thông tin được chèn vào này được gọi là Extension Header. Như vậy ngoài ý nghĩa như trường Protocol của IPv4 thì trường Next Header còn cho biết Extension Header nào đang được chèn thêm vào.

Những trường không còn giữ lại:

Internet Header Length (IHL)

Do chiều dài Header của IPv4 không cố định nên cần sử dụng IHL để mô tả. Trường này cùng với Total Length nhằm xác định chiều dài của phần Payload. Với IPv6, chiều dài của phần Header cố định là 40 byte nên trường IHL này không còn được sử dụng.



Hình 24. Những trường của IPv4 được giữ lại và bị xóa bỏ khỏi IPv6

Indentification, Flags và Fragment Offset

Trong IPv4, ba trường Identification, Flags và Fragment Offset hỗ trợ phân mảnh bản tin khi kích thước vượt quá MTU (Maximum Transmission Unit). Identification (16 bit) giúp xác định các bản tin phân mảnh thuộc cùng một bản tin gốc. Fragment Offset (13 bit) chỉ thứ tự sắp xếp của các bản tin bị phân mảnh. Flags (3 bit) báo trạng thái: cấm phân mảnh (DF), còn bản tin phân mảnh tiếp theo (More Fragments=1), hay bản tin cuối (More Fragments=0).

Trong IPv6, ba trường này không nằm trong header chính mà được chuyển vào Extension Header, chỉ xuất hiện khi phân mảnh xảy ra. Khác với IPv4, thiết bị trung gian không phân mảnh mà thông báo MTU về nguồn (Source). Nguồn tự điều chỉnh, phân mảnh bản tin theo MTU và truyền lại. Cách này giảm tải cho router và tối ưu xử lý.

Header Checksum

Trường này giúp kiểm tra gói tin có bị lỗi trong quá trình truyền dữ liệu hay không. Tất cả các Router tham gia quá trình truyền dữ liệu đều kiểm tra trường này, nếu phát hiện lỗi thì loại bỏ bản tin. Một số giao thức ở lớp 2 như Ethernet đã sẵn có trường kiểm tra toàn vẹn dữ liệu CRC (Cyclic Redundancy Check) hoặc giao thức lớp 3 như TCP và UDP cũng có trường Checksum. Chính vì thế giao thức IPv6 không giữ lại trường này nhằm bỏ bớt sự trùng lặp quá trình kiểm tra lỗi. Trường Checksum luôn có trong bản tin TCP của IPv4 còn trong UDP thì là tùy chọn. Chuyển sang IPv6, trường Checksum của UDP bắt buộc phải có nhằm hỗ trợ cho tính năng Checksum bị loại bỏ trong bản tin IPv6.

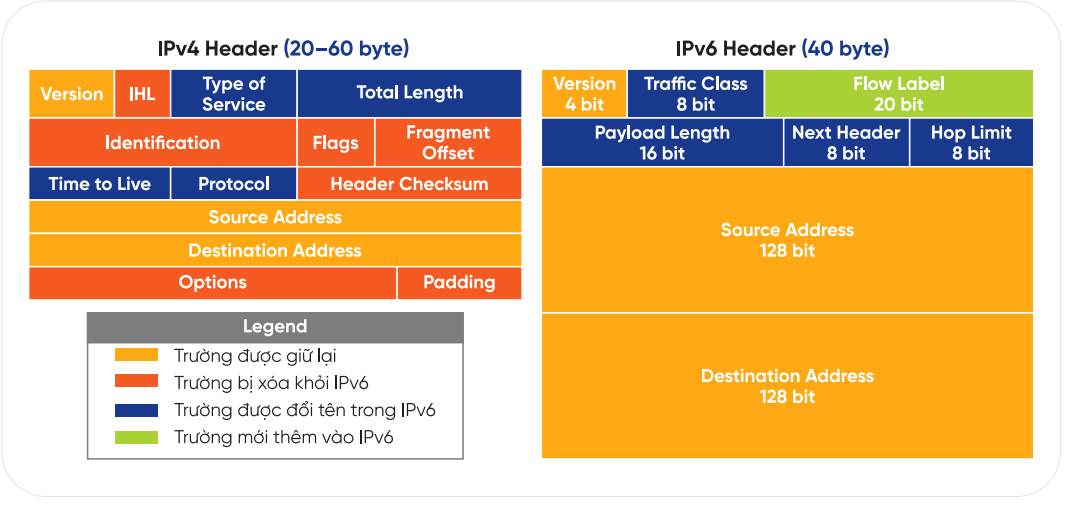
Options và Padding

Đây là hai trường tùy chọn nên có thể có hoặc không xuất hiện trong IPv4. Options cho phép thực hiện một số chức năng như ghi lại thời gian gói tin đi qua (TimeStamp), những Router đã đi qua (Record Route), ... Mục Padding dùng cùng với Options nhằm thêm các ký tự 0 để bảo đảm phần Header luôn là bội số của 32 bit. Các trường này cũng được đưa vào phần Extension Header.

Trường mới trong IPv6:

Flow label:

Trường 20 bit này dùng để xác định những bản tin nào thuộc cùng một luồng dữ liệu (Flow), qua đó giúp các Router có cách xử lý chung cho các bản tin cùng nhãn Flow. Khi Router nhận một bản tin có nhãn sẽ thực hiện một số thủ tục xử lý trước khi chuyển tiếp bản tin, những bản tin tiếp sau nếu có cùng nhãn sẽ được giảm bớt các thủ tục và chuyển tiếp nhanh chóng hơn.

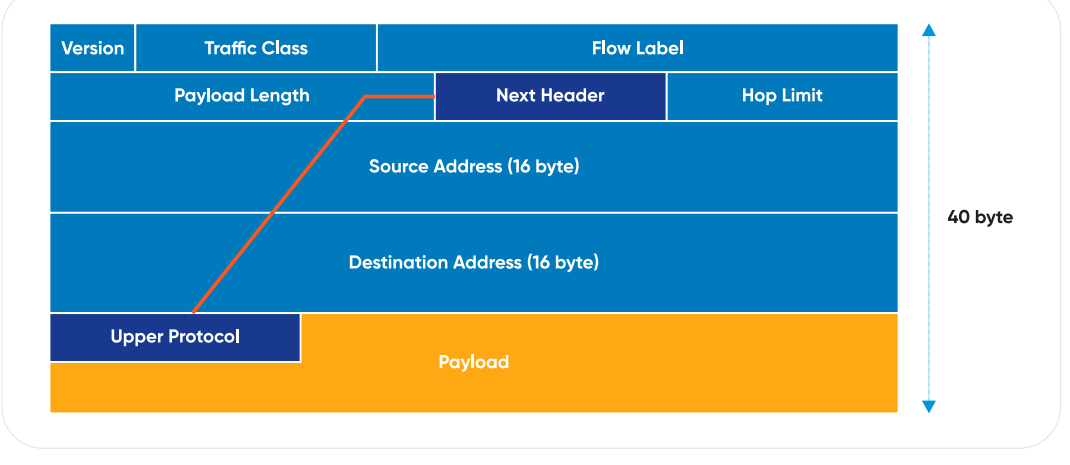


Hình 25. Chi tiết các trường của IPv6

2.3 TIÊU ĐỀ MỞ RỘNG (EXTENSION HEADER)

Giao thức IPv4, với các trường như Options, Padding và những trường liên quan đến phân mảnh gói tin, dẫn đến kích thước tiêu đề biến động từ 20 đến 60 byte, gây phức tạp trong thiết kế. IPv6 khắc phục hạn chế này bằng cách loại bỏ các trường trên, cố định kích thước tiêu đề ở mức 40 byte, như đã trình bày. Các chức năng của những trường bị loại bỏ được tích hợp vào một cơ chế mới trong IPv6, gọi là **tiêu đề mở rộng (Extension Header)**. Cơ chế này không chỉ duy trì các chức năng cũ mà còn bổ sung những tính năng tiên tiến, tối ưu hóa quá trình truyền tải gói tin IPv6.

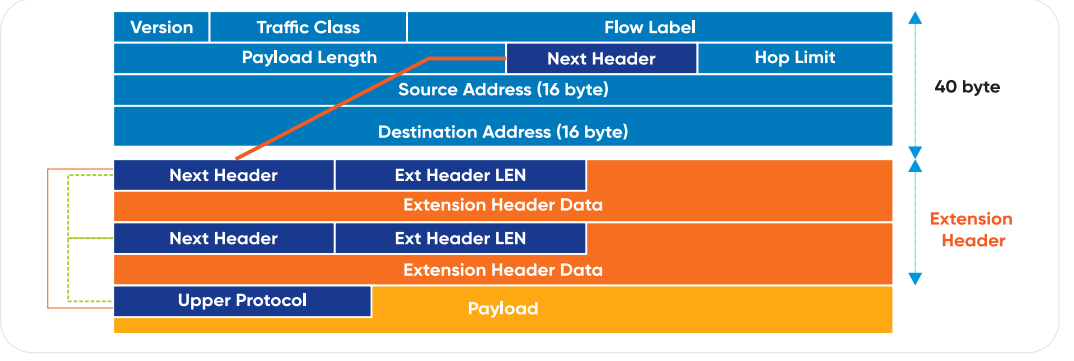
Tiêu đề mở rộng mang tính **tùy chọn**, chỉ được sử dụng khi cần thiết, đảm bảo tính linh hoạt và hiệu quả. IPv6 hỗ trợ nhiều loại tiêu đề mở rộng, phần lớn được xử lý bởi **node đích**, trong khi chỉ một số ít được các **Router** trên đường truyền xử lý, tối ưu hóa hiệu suất truyền tải.



Hình 26. Ý nghĩa của trường Next Header

Trong trường hợp không sử dụng tiêu đề mở rộng, trường Next Header trong IPv6 (tương ứng với trường Protocol trong IPv4) xác định giao thức tầng trên (Upper Protocol) được gói tin IPv6 truyền tải, chẳng hạn như TCP (giá trị 6), UDP (17), ICMPv6 (58), VRRPv3 (112), OSPFv3 (89), GRE (47)... Các giá trị này được giữ nguyên từ IPv4, đảm bảo tính tương thích.

Khi cần thực hiện các chức năng bổ sung, chẳng hạn như phân mảnh gói tin, một tiêu đề mở rộng sẽ được chèn giữa **tiêu đề chính (Main Header)** và phần dữ liệu (Payload). Lúc này, trường **Next Header** trong tiêu đề chính sẽ chỉ định loại **tiêu đề mở rộng** được sử dụng, cho phép hệ thống xác định và xử lý chính xác các chức năng mở rộng theo yêu cầu.



Hình 27. Vị trí của Extension Header

Trong một gói tin IPv6, có thể tồn tại nhiều tiêu đề mở rộng được chèn nối tiếp nhau (Chain) để đáp ứng các chức năng khác nhau. Mỗi tiêu đề mở rộng chứa một trường Next Header, cho phép xác định loại tiêu đề mở rộng tiếp theo hoặc giao thức của phần dữ liệu (Payload) nếu không còn tiêu đề mở rộng nào. Trường Next Header trong tiêu đề mở rộng cuối cùng luôn chỉ định giao thức của Payload, chẳng hạn như TCP, UDP, ICMPv6, hoặc các giao thức khác, đảm bảo tính liên tục và chính xác trong quá trình xử lý gói tin.

Có thể thấy tiêu đề mở rộng đóng vai trò quan trọng trong IPv6, không chỉ giúp cố định kích thước tiêu đề chính ở mức 40 byte mà còn tăng cường khả năng linh hoạt bằng cách bổ sung các tính năng mới cho việc truyền tải và xử lý gói tin. Thiết kế này đảm bảo rằng các tính năng trong tương lai có thể được tích hợp mà không làm thay đổi cấu trúc cốt lõi của gói tin IPv6, duy trì tính mở rộng và bền vững của giao thức.

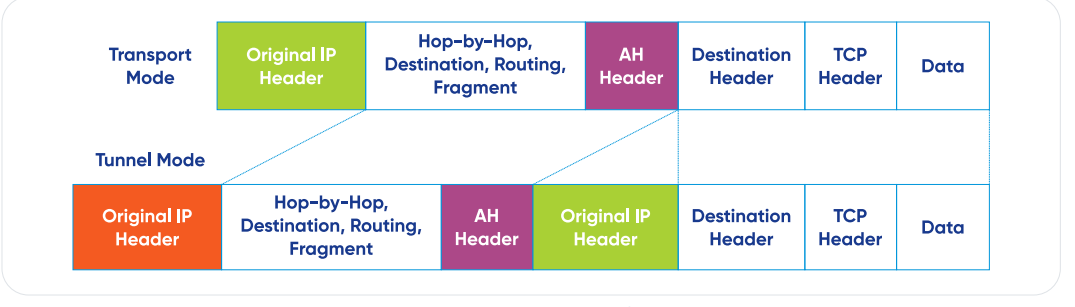
Có nhiều loại tiêu đề mở rộng để phục vụ các chức năng khác nhau. Do một gói tin có thể chứa nhiều tiêu đề mở rộng, việc quy định thứ tự xử lý là cần thiết để đảm bảo hiệu quả và nhất quán. Dưới đây là những tiêu đề mở rộng phổ biến nhất và các mã Next Header tương ứng.

MÃ NEXT HEADER	TÊN HEADER/ EXTENSION HEADER	THỨ TỰ	MỤC ĐÍCH
	IPv6 Main Header	1	Tiêu đề chính của bản tin IPv6
0	Hop-by-Hop Options	2	Yêu cầu các Router dọc tuyến phải xử lý bản tin
60	Destination Options	3	Kết hợp với Routing Header, yêu cầu các node có trong Routing Header phải xử lý bản tin
43	Routing Header	4	Chỉ định những node mạng mà bản tin cần phải đi qua, không phụ thuộc vào Routing Table của các Router
44	Fragment Header	5	Phục vụ phân mảnh các bản tin
51	Authentication Header	6	Xác thực bản tin như IPSec
50	Encapsulation Security Payload Header	7	Mã hóa bản tin như IPSec
60	Destination Options	8	Không kết hợp với Routing Header, chỉ yêu cầu node đích phải xử lý bản tin
135	Mobility Header	9	Cho phép node mạng khi chuyển sang mạng khác vẫn giữ kết nối với mạng cũ
59	No next header		Bỏ qua không kiểm tra các thông tin sau phần Header có chứa mã này và truyền bản tin nguyên vẹn

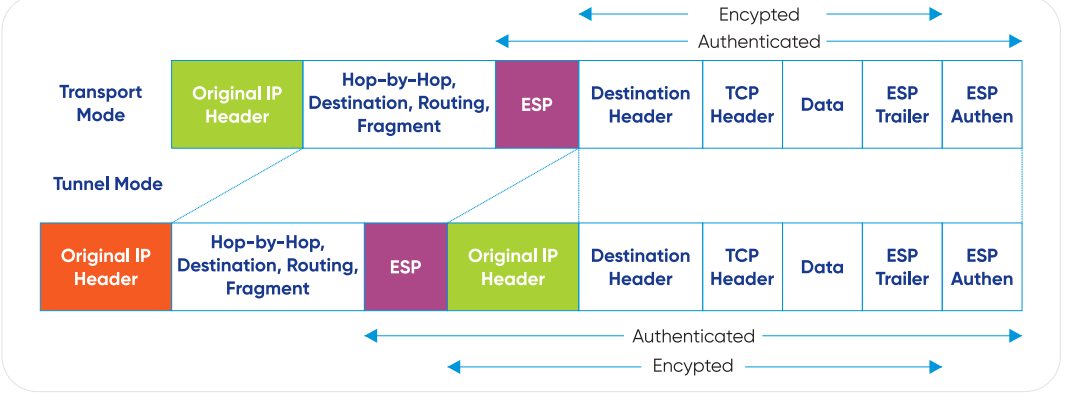
Bảng 2. Một số Extension Header phổ biến

Sau đây là vài đặc điểm đáng chú ý của một số tiêu đề mở rộng:

- **Hop-by-Hop Options Header (Next Header: 0):** Đây là tiêu đề mở rộng duy nhất yêu cầu tất cả router trên đường truyền phải xử lý, hỗ trợ các tùy chọn đặc biệt như kiểm tra hoặc tối ưu hóa lộ trình tại mỗi hop. Điều này đảm bảo gói tin được xử lý linh hoạt trong suốt hành trình truyền tải.
- **Destination Options Header (Next Header: 60):** Tiêu đề này chứa các tùy chọn chỉ được xử lý bởi node đích hoặc các node được chỉ định trong lộ trình. Điểm nổi bật là nó có thể xuất hiện hai lần trong một gói tin IPv6, với các vị trí khác nhau trong chuỗi tiêu đề, phục vụ các mục đích xử lý riêng biệt, chẳng hạn như cung cấp thông tin bổ sung cho node đích hoặc node trung gian.
- **Routing Header (Next Header: 43):** Cho phép node nguồn chỉ định danh sách các node trung gian mà gói tin phải đi qua, bỏ qua các bảng định tuyến thông thường của router. Tiêu đề này thường kết hợp với Destination Options Header để xác định chính xác các node trung gian, mang lại khả năng kiểm soát lộ trình nâng cao.
- **Fragment Header (Next Header: 44):** Đóng vai trò quan trọng trong việc giữ kích thước tiêu đề chính cố định ở 40 byte, tiêu đề này hỗ trợ phân mảnh gói tin. Khác với IPv4, nơi router trung gian thực hiện phân mảnh, IPv6 yêu cầu node nguồn đảm nhiệm toàn bộ quá trình này. Cơ chế phân mảnh tương tự IPv4 nhưng được tối ưu để giảm tải cho router trung gian, chi tiết sẽ được trình bày sau.
- **Authentication Header (AH) (Next Header: 51) và Encapsulating Security Payload Header (ESP) (Next Header: 50):** Hai tiêu đề này tích hợp các tính năng bảo mật của IPSec trực tiếp vào IPv6. AH đảm bảo xác thực và tính toàn vẹn dữ liệu, trong khi ESP bổ sung mã hóa để bảo vệ nội dung Payload. Cả hai hỗ trợ Tunnel Mode (bảo vệ toàn bộ gói tin) và Transport Mode (bảo vệ Payload), mang lại sự linh hoạt và bảo mật tối ưu.
- **Xử lý lỗi tiêu đề mở rộng:** Khi một Router nhận được một Extension Header lỗi hoặc không xác định, gói tin IPv6 sẽ bị loại bỏ. Đồng thời, một bản tin ICMPv6 với Type=4, Code=1 (unrecognized Next Header type encountered) sẽ được gửi trả về node nguồn, thông báo về vấn đề gặp phải. Cơ chế này đảm bảo khả năng phát hiện và xử lý lỗi hiệu quả, duy trì tính ổn định của quá trình truyền tải.



Hình 28. Vị trí AH và các Extension Header khác ở chế độ Transport và Tunnel



Hình 29. Vị trí ESP và các Extension Header khác ở chế độ Transport và Tunnel

Những đặc điểm này không chỉ thể hiện tính linh hoạt và mạnh mẽ của kiến trúc tiêu đề mở rộng trong IPv6 mà còn đảm bảo khả năng mở rộng trong tương lai. Thiết kế này cho phép tích hợp các tính năng mới mà không làm thay đổi cấu trúc cốt lõi của giao thức, đồng thời cung cấp cơ chế xử lý lỗi chặt chẽ để duy trì hiệu suất và độ tin cậy của mạng.

2.4 TỔNG KẾT CHƯƠNG 2

Chương 2 đã cung cấp cái nhìn toàn diện về giao thức IPv6, làm nổi bật những cải tiến vượt trội so với IPv4, từ việc giải quyết vấn đề cạn kiệt địa chỉ đến việc thiết kế một kiến trúc hiện đại, hiệu quả và bền vững. Những đặc điểm kỹ thuật ưu việt của IPv6, đặc biệt là cấu trúc bản tin, đã tạo động lực mạnh mẽ cho các nhà mạng, tổ chức và doanh nghiệp chuyển đổi sang giao thức này để đáp ứng nhu cầu ngày càng cao của mạng lưới toàn cầu.

IPv6 không chỉ là giải pháp thay thế IPv4 mà còn là nền tảng cho sự phát triển bền vững của mạng Internet. Để tìm hiểu chi tiết hơn về định dạng và hoạt động của giao thức, bạn đọc có thể tham khảo tài liệu chuẩn quốc tế **RFC 8200 – Internet Protocol, Version 6 (IPv6) Specification** và **RFC 2460**, nơi cung cấp thông tin chuyên sâu về các đặc điểm kỹ thuật của IPv6.

2.5 CÂU HỎI ÔN TẬP CHƯƠNG 2

01 Tại sao việc chuyển đổi từ IPv4 sang IPv6 vì vấn đề cạn kiệt địa chỉ IPv4 chỉ là một phần của lý do?

Địa chỉ IPv4 có giới hạn về số lượng, trong khi IPv6 cung cấp một không gian địa chỉ gần như vô hạn, giải quyết triệt để vấn đề cạn kiệt. Tuy nhiên, lý do chính để chuyển đổi là kiến trúc được cải tiến và các tính năng bổ sung của IPv6, giúp nâng cao hiệu suất, bảo mật và khả năng mở rộng của mạng.

02 IPv6 khác biệt như thế nào so với IPv4 trong cấu trúc tiêu đề bản tin (Header)?

Tiêu đề IPv6 có kích thước cố định là 40 byte, đơn giản hơn và có ít trường hơn so với tiêu đề IPv4 (20-60 byte). Một số trường của IPv4 được giữ lại (Version, Source/Destination Address), một số được đổi tên (Type of Service thành Traffic Class, Total Length thành Payload Length, Time-to-live thành Hop Limit, Protocol thành Next Header), một số bị loại bỏ (IHL, Identification, Flags, Fragment Offset, Header Checksum, Option, Padding)và một trường mới được thêm vào (Flow Label). Đặc biệt, IPv6 giới thiệu Tiêu đề mở rộng (Extension Header) để cung cấp thêm tính năng một cách linh hoạt.

03 Vai trò của trường "Next Header" trong tiêu đề IPv6 là gì?

Trường "Next Header" trong tiêu đề chính của IPv6 có vai trò tương tự như trường "Protocol" trong IPv4, xác định giao thức lớp trên (ví dụ: TCP, UDP) nằm trong phần dữ liệu (Payload). Ngoài ra, nếu có Tiêu đề mở rộng được chèn vào giữa tiêu đề chính và Payload, trường "Next Header" sẽ chỉ định loại Tiêu đề mở rộng tiếp theo. Trong các Tiêu đề mở rộng được xếp chồng, trường "Next Header" trong mỗi tiêu đề sẽ trỏ đến tiêu đề mở rộng kế tiếp hoặc đến Payload.

04 Tiêu đề mở rộng (Extension Header) trong IPv6 là gì và chúng mang lại lợi ích gì?

Tiêu đề mở rộng là một phần tùy chọn trong bản tin IPv6, được chèn sau tiêu đề chính và trước phần dữ liệu. Chúng cho phép thêm các chức năng bổ sung vào giao thức IPv6 mà không làm thay đổi cấu trúc tiêu đề cơ bản. Các chức năng này bao gồm xử lý tùy chọn (Hop-by-Hop Options, Destination Options), định tuyến đặc biệt (Routing Header), phân mảnh (Fragment Header), bảo mật (Authentication Header, Encapsulation Security Payload Header), hỗ trợ di động (Mobility Header)... Việc sử dụng Tiêu đề mở rộng giúp tiêu đề chính của IPv6 có kích thước cố định và cho phép mở rộng tính năng của giao thức trong tương lai mà không cần thay đổi cấu trúc cơ bản.

05 Những giao thức nào hỗ trợ IPv6 và có sự khác biệt nào so với các giao thức hỗ trợ IPv4?

IPv6 được thiết kế để hoạt động song song với IPv4 trong bộ giao thức TCP/IP mà không làm ảnh hưởng đến các giao thức ở các tầng khác như TCP và UDP. Tuy nhiên, một số giao thức hỗ trợ IPv4 đã được thay thế hoặc cập nhật để phù hợp với IPv6. Ví dụ, ARP được thay thế bằng NDP (Neighbor Discovery Protocol), IGMP được thay thế bằng MLD (Multicast Listener Discovery), trong khi ICMP được cập nhật thành ICMPv6, OSPF được cập nhật thành OSPFv3 (RIPng, BGP4 cũng được cập nhật). Các giao thức này được cải tiến dựa trên kinh nghiệm từ IPv4 để hoạt động hiệu quả hơn với IPv6.

06 Việc phân mảnh gói tin được xử lý như thế nào trong IPv6 so với IPv4?

Trong IPv4, các Router trung gian có thể thực hiện phân mảnh gói tin nếu kích thước gói tin vượt quá MTU (Maximum Transmission Unit) của đường truyền. Ngược lại, IPv6 loại bỏ khả năng này ở các Router trung gian. Thay vào đó, IPv6 yêu cầu thiết bị nguồn tự động phát hiện MTU của đường truyền (Path MTU Discovery) và tự phân mảnh gói tin trước khi gửi đi nếu cần thiết. Thông tin về phân mảnh được chứa trong Tiêu đề mở rộng Fragment.

07 Tại sao trường "Header Checksum" bị loại bỏ khỏi tiêu đề IPv6?

Trường "Header Checksum" trong IPv4 được sử dụng để kiểm tra lỗi trong quá trình truyền dữ liệu của tiêu đề IP. Tuy nhiên, các giao thức ở tầng liên kết dữ liệu (ví dụ: Ethernet với CRC) và tầng giao vận (TCP, UDP với Checksum) đã cung cấp cơ chế kiểm tra lỗi. Để tránh sự trùng lặp và tăng hiệu suất, trường "Header Checksum" đã bị loại bỏ khỏi tiêu đề IPv6. Đáng chú ý, trường Checksum trở thành bắt buộc trong UDP khi sử dụng IPv6.

08 Trường "Flow Label" trong tiêu đề IPv6 có chức năng gì?

Trường "Flow Label" là một trường 20 bit trong tiêu đề IPv6, được sử dụng để xác định các gói tin thuộc cùng một "luồng" dữ liệu (Flow). Điều này cho phép các router có thể nhận diện và áp dụng cùng một chính sách xử lý (ví dụ: chất lượng dịch vụ - QoS) cho tất cả các gói tin thuộc cùng một luồng, giúp tăng tốc độ chuyển tiếp và cải thiện hiệu suất mạng cho các ứng dụng yêu cầu băng thông hoặc độ trễ thấp.

PHẦN 1 – LÝ THUYẾT

CHƯƠNG 3

CHI TIẾT CÁC LOẠI ĐỊA CHỈ IPv6

CHƯƠNG 3

CHI TIẾT CÁC LOẠI ĐỊA CHỈ IPv6

Trong mô hình TCP/IP, địa chỉ IP đóng vai trò rất quan trọng, ảnh hưởng trực tiếp đến các hoạt động như quy hoạch địa chỉ, cấu hình thiết bị, cung cấp dịch vụ, giám sát và xử lý sự cố. Do đó, việc nắm vững cấu trúc, đặc tính và cơ chế hoạt động của địa chỉ IPv6 là yêu cầu không thể thiếu để vận hành hiệu quả hệ thống mạng thế hệ mới này. Phần tiếp theo, chương 3, sẽ tập trung phân tích chi tiết các đặc điểm kỹ thuật của địa chỉ IPv6, bao gồm cách biểu diễn, phân loại và các quy tắc liên quan, nhằm cung cấp nền tảng vững chắc cho người đọc.

Chương 3 mở đầu bằng việc nhấn mạnh tầm quan trọng của địa chỉ IP trong mô hình TCP/IP và sự cần thiết phải nắm vững kiến thức về địa chỉ IPv6. Tiếp đó, đi sâu vào cách biểu diễn địa chỉ IPv6, so sánh với IPv4 và giới thiệu các loại địa chỉ IPv6 khác nhau, bao gồm Unicast (với các loại địa chỉ GUA, ULA, LLA), Multicast và Anycast, đồng thời làm rõ các nguyên tắc lựa chọn địa chỉ nguồn khi có nhiều địa chỉ khả dụng. Mục tiêu chính của chương là cung cấp nền tảng vững chắc về các khái niệm địa chỉ IPv6 để người đọc có thể hiểu và vận hành hiệu quả hệ thống mạng thế hệ mới.

NHỮNG NỘI DUNG CỦA CHƯƠNG 3 GỒM:

Thông tin chi tiết về **các loại địa chỉ IPv6**, bao gồm cấu trúc, đặc tính và cơ chế hoạt động của chúng.

Cách biểu diễn địa chỉ IPv6 và các cải tiến giúp thuận tiện cho việc đọc và viết so với IPv4. Bạn sẽ hiểu tại sao hệ Hexa được lựa chọn và cách các địa chỉ 128 bit được chia thành 8 phần (Hextet).

Các **quy tắc viết rút gọn** địa chỉ IPv6 theo RFC 5952, bao gồm việc rút gọn số 0 ở bên trái, cụm bốn số 0 và nhiều cụm bốn số 0 liên tiếp bằng dấu "::".

Phân loại địa chỉ IPv6 theo cách thức hoạt động (Type) và phạm vi hoạt động (Scope).

Chi tiết về từng loại **địa chỉ Unicast**: Địa chỉ Global Unicast (GUA), Unique Local (ULA), Link Local (LLA), Unspecified (::/128), Loopback (::1/128) và IPv4 Embedded.

Chi tiết về **địa chỉ Multicast**, bao gồm địa chỉ Well-known Multicast và địa chỉ Solicited-Node Multicast.

Hiểu các **quy tắc lựa chọn** địa chỉ IPv6 (cả nguồn và đích) khi một Interface có nhiều địa chỉ

Bảng **Policy Table** theo RFC 6724 và vai trò của Precedence và Label trong việc ưu tiên lựa chọn địa chỉ.

3.1. CÁCH BIỂU DIỄN ĐỊA CHỈ IPv6

Ấn tượng đầu tiên đối với địa chỉ IPv6 là cách biểu diễn hoàn toàn khác biệt so với IPv4. Với độ dài 128 bit, việc sử dụng hệ thập phân để biểu diễn sẽ tạo ra chuỗi số quá dài và phức tạp. Do đó, hệ thập lục phân (Hexadecimal) được chọn làm chuẩn cho IPv6, kết hợp với các cải tiến nhằm đơn giản hóa việc đọc và ghi địa chỉ. Nội dung dưới đây sẽ trình bày cấu trúc, cách biểu diễn và đặc điểm của địa chỉ IPv6, so sánh với IPv4 để làm rõ những điểm khác biệt.

Địa chỉ IPv6 được chia thành 8 phần, mỗi phần dài 16 bit, được gọi là **Hextet**. Các Hextet được phân tách bằng dấu hai chấm ":", thay vì dấu chấm "." như trong IPv4. Mỗi Hextet được viết dạng ký tự hệ Hexadecimal, bao gồm các số từ 0 đến 9 và chữ cái từ A đến F, tạo nên một định dạng gọn gàng và dễ nhận diện hơn.

ĐỊA CHỈ IPv4	ĐỊA CHỈ IPv6
Là địa chỉ có độ dài **32 bit**	Là địa chỉ có độ dài **128 bit**
Được chia làm **4 phần 8 bit** (Octet)	Địa chỉ chia làm **8 phần 16 bit** (hextet)
Viết dưới dạng **thập phân** (chỉ có số)	Viết dưới dạng **Hexa** (gồm số và chữ)
Cách nhau bởi dấu chấm (.)	Cách nhau bởi dấu hai chấm :
Viết **đầy đủ**	Cách viết có thể **rút gọn**

Bảng 3. Đặc điểm của địa chỉ IPv6

Sau đây xét một địa chỉ IPv6 được biểu diễn ở các dạng khác nhau để thấy tại sao hệ Hexa được lựa chọn:

128 bit dạng nhị phân (Binary)

00100000000000010000110110111000101011000001000000000000000000000100010100001011100000000000000000000000000000000000000011010010100101

128 bit dạng thập phân (Decimal)

42540766464533357369246066665274219090 (38 chữ số)

Dạng thập phân theo nhóm 8 bit như IPv4

32:1:13:184:172:16:0:0:138:46:0:0:0:0:26:82

Dạng thập phân theo nhóm 16 bit như IPv4

8193:3512:44048:0:35374:0:0:6738

Dạng thập lục phân (Hexa) theo nhóm 16 bit

2001:0db8:ac10:0000:8a2e:0000:0000:1a52

Có thể thấy rằng cách biểu diễn theo hệ Hexa là cách viết tối ưu nhất so với các dạng khác, mỗi phần tối đa chỉ có 4 ký tự và không quá dài. Mặt khác chúng ta cũng đã từng quen với cách biểu diễn dạng Hexa này qua địa chỉ MAC của các cổng mạng nên dễ dàng làm quen với cách biểu diễn theo hệ Hexa của IPv6.

Không chỉ dừng lại ở hệ Hexa, IPv6 có điểm rất đặc biệt là cho phép viết rút gọn nên trong thực tế địa chỉ IPv6 sẽ biểu diễn dài ngắn khác nhau, không cố định bốn phần như IPv4. Hãy xét minh họa một địa chỉ IPv6 đầy đủ theo hệ Hexa.

2001:0db8:ac10:0000:8a2e:0000:0000:1a52

Để viết rút gọn thì RFC 5952 đã quy định một số nguyên tắc sau:

- **Số 0 bên trái:** Được rút gọn
- **Cụm bốn số 0:** Viết thành một số 0
- **Nhiều "cụm bốn số 0" liên tiếp:** Thay bằng dấu "::"
- **Dấu ::** chỉ được viết 01 lần

Hình 30. Minh họa cách viết rút gọn địa chỉ IPv6

Nếu "cụm bốn số 0" xuất hiện nhiều lần thì tuân theo nguyên tắc:

- Cụm nào nhiều số 0 hơn: sẽ được thay thế bằng ::
- Nếu bằng nhau: thì cụm bên trái được thay bằng ::

Những nguyên tắc rút gọn này giúp địa chỉ IPv6 được biểu diễn rất gọn gàng và dễ nhớ trong nhiều trường hợp. Đây là điểm rất tối ưu của địa chỉ IPv6.

3.2. PHÂN LOẠI ĐỊA CHỈ IPv6

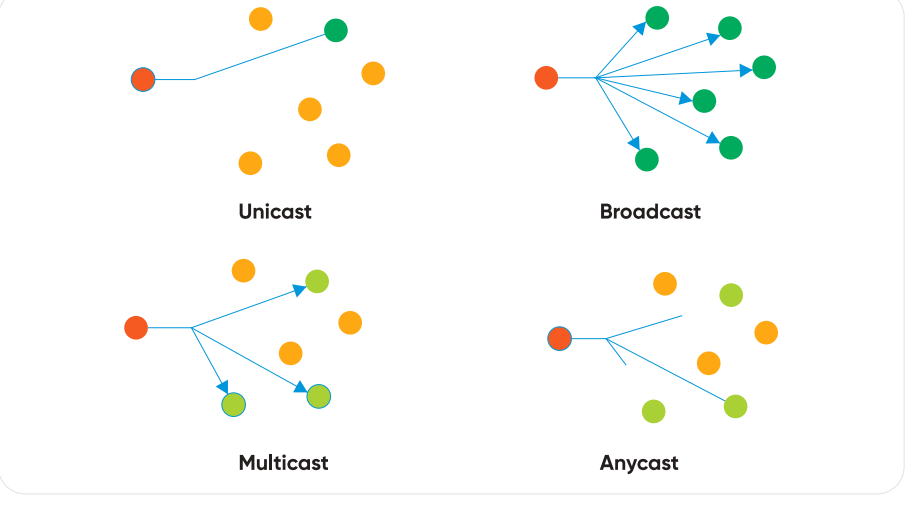
Cũng như IPv4, địa chỉ IPv6 không chỉ có một loại duy nhất mà được phân loại thành các nhóm. Cách phân loại IPv6 phần lớn kế thừa từ IPv4 chỉ có một vài điểm khác nhau nhằm tối ưu hơn. Hai cách phân loại chính của IPv4 và IPv6 là cách thức (Type) và phạm vi (Scope) hoạt động.

Phân loại theo kiểu truyền dữ liệu (Type):

Theo cách này thì địa chỉ IPv4 và IPv6 có bốn kiểu truyền chính là Unicast, Multicast, Broadcast và Anycast, đặc điểm của mỗi loại như sau:

Unicast:

Khi một gói tin có địa chỉ đích là Unicast thì gói tin đó chỉ được gửi đến cổng mạng có địa chỉ tương ứng. Cách truyền dữ liệu dùng địa chỉ Unicast được gọi là kiểu truyền **"một-đến-một"** (One-to-One) đây là cách truyền phổ biến nhất trong thực tế.



Hình 31. Cách thức hoạt động của các loại địa chỉ

Multicast

Khi một bản tin có đích là địa chỉ Multicast thì có nhiều thiết bị cùng nhận bản tin này. Cách truyền dữ liệu này gọi là **"một-đến-nhiều" (1 - to - multiple)** và thường được áp dụng cho dịch vụ truyền hình qua mạng (IPTV hoặc Broadcast TV) và trong một số giao thức định tuyến như OSPF, RIP.

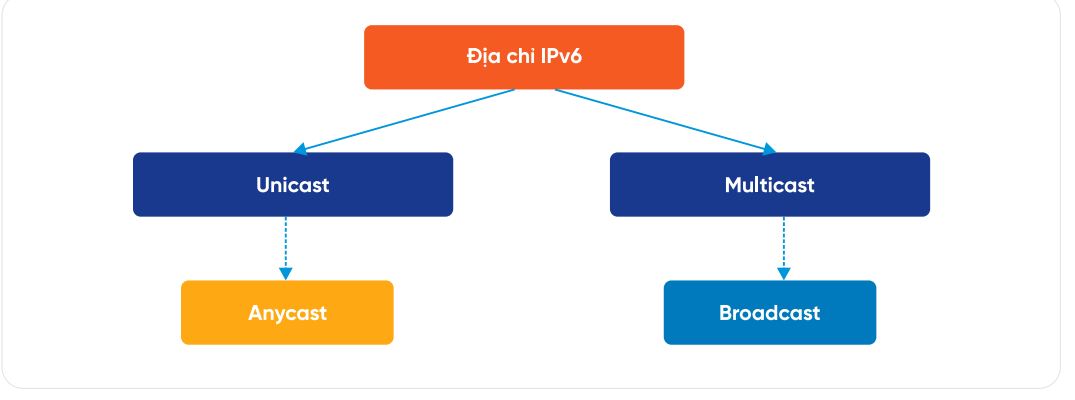
Broadcast

Kiểu truyền này tương ứng với mô hình **"một-đến-tất cả" (1-to-all)**. Các thiết bị nếu nhận được bản tin Broadcast đều phải kiểm tra xem bản tin có liên quan đến mình hay không, nếu có thì xử lý các bước tiếp theo còn không thì loại bỏ bản tin. Vì thế các bản tin Broadcast thường gây ảnh hưởng rất nhiều đến hoạt động của mạng và các thiết bị.

Anycast

Là đại diện cho một nhóm các máy tính nhưng chỉ có một máy tính nhận được bản tin gửi đến thay vì cả nhóm như Multicast. Cách thức hoạt động của Unicast là nhiều máy tính ở các vị trí mạng khác cùng dùng chung một địa chỉ và máy tính nào gần địa chỉ nguồn nhất sẽ được chọn là đích. Cách truyền này gọi là **"một đến một trong những" (1 to 1 of)**. Trong thực tế địa chỉ các DNS Server như 8.8.8.8, 1.1.1.1 ... đều là địa chỉ Anycast vì các địa chỉ này được gán cho nhiều Server nằm rải rác ở khắp nơi trên toàn thế giới.

Trong bốn loại địa chỉ trên, Anycast thực sự là địa chỉ Unicast được dùng cho nhiều cổng mạng chứ không có quy định cách biểu diễn hay được quy hoạch riêng. Các địa chỉ còn lại điều có quy định riêng cho mỗi loại. IPv4 có quy định riêng cho Broadcast nhưng IPv6 thì không mà thay vào đó sử dụng một địa chỉ IPv6 Multicast đặc biệt để đại diện địa chỉ Broadcast. Đây là điều hay nhầm lẫn về địa chỉ Broadcast IPv6. Có nghĩa là **kiểu truyền theo cách Broadcast** không mất đi trong IPv6 mà chỉ có cách biểu diễn dành riêng cho địa chỉ Broadcast không còn và thay bằng một địa chỉ Multicast đặc biệt. Dưới đây là minh họa cho các loại địa chỉ phân theo cách thức hoạt động của IPv6.



Hình 32. Phân loại địa chỉ IPv6 theo cách thức hoạt động

Phân loại theo phạm vi hoạt động (Scope):

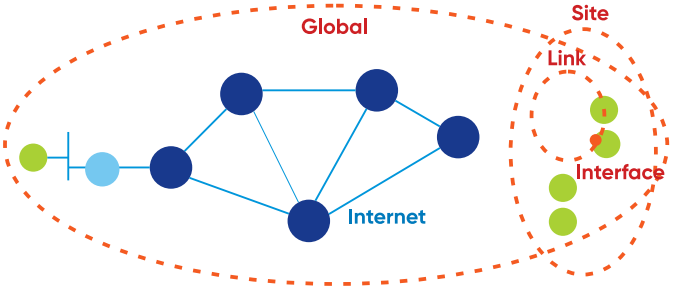
Phạm vi hoạt động có nghĩa là không gian mà địa chỉ có ý nghĩa hay truy cập được. IPv4 gồm hai loại là địa chỉ công cộng Public và địa chỉ nội bộ Private nhưng IPv6 có đến ba loại:

Địa chỉ Global Unicast (GUA):

Địa chỉ này có phạm vi toàn cầu giống như Public của IPv4, là địa chỉ thường dùng nhất trong thực tế.

Địa chỉ Unique Local (ULA)

Địa chỉ tương tương ứng với IPv4 Private, chỉ có phạm vi nội bộ nên bị loại bỏ trên mạng Internet. Do IPv6 có không gian địa chỉ lớn nên địa chỉ GUA thường được dùng thay cho ULA. Một phần nữa do việc chuyển đổi địa chỉ NAT (Network Address Translation) gây vấn đề đối với một số ứng dụng nên đã bị loại bỏ trong IPv6, vì thế địa chỉ ULA ít được dùng.



Hình 33. Phân loại địa chỉ IPv6 theo phạm vi hoạt động

Địa chỉ Link Local (LLA):

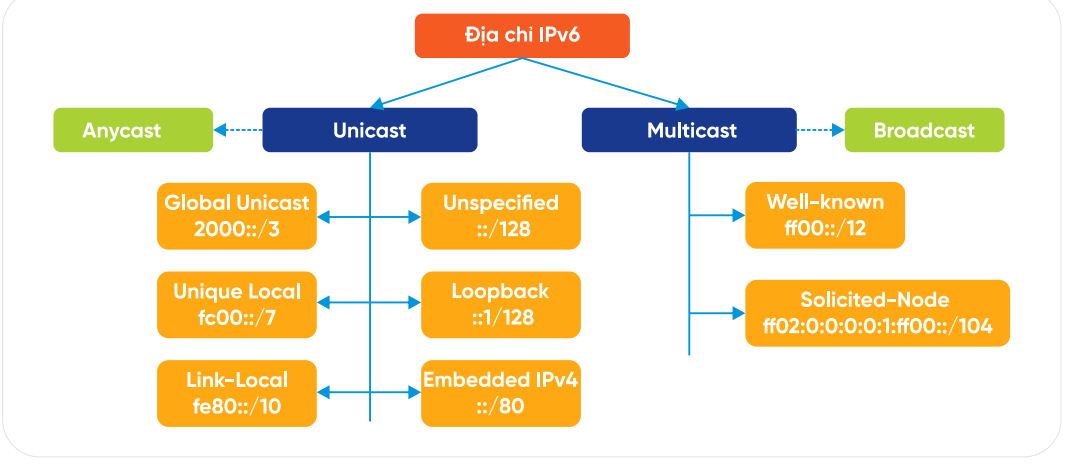
Đây là địa chỉ mới không có địa chỉ tương đương trong IPv4. Phạm vi của địa chỉ này là chỉ trong cùng một phân đoạn mạng (Segment) như cùng VLAN. Địa chỉ này không được định tuyến nên Router sẽ không chuyển tiếp những bản tin có đích là địa chỉ này sang các cổng giao diện khác.

Chú ý:

- IPv4 chỉ có khái niệm Scope cho địa chỉ Unicast còn IPv6 thì cho cả Multicast nhưng Scope được dùng phổ biến là Link Local Multicast, sẽ được trình bày sau.
- Ngoài các cách phân loại như trên thì có một số loại đặc biệt khác như Unicast có địa chỉ Loopback, Unspecified hoặc Embedded dùng cho các mục đích cụ thể. Địa chỉ Multicast cũng được chia làm hai loại chính là Well-known và Solicited-Node.
- Mỗi loại địa chỉ được phân loại sẽ có đặc điểm và quy định riêng.

3.3. VỊ TRÍ PHÂN VÙNG CÁC LOẠI ĐỊA CHỈ IPv6

Kết hợp hai cách phân loại ở trên chúng ta có sơ đồ tổng quan mô tả các loại địa chỉ IPv6 như sau. Chi tiết từng loại địa chỉ sẽ trình bày ở phần sau.

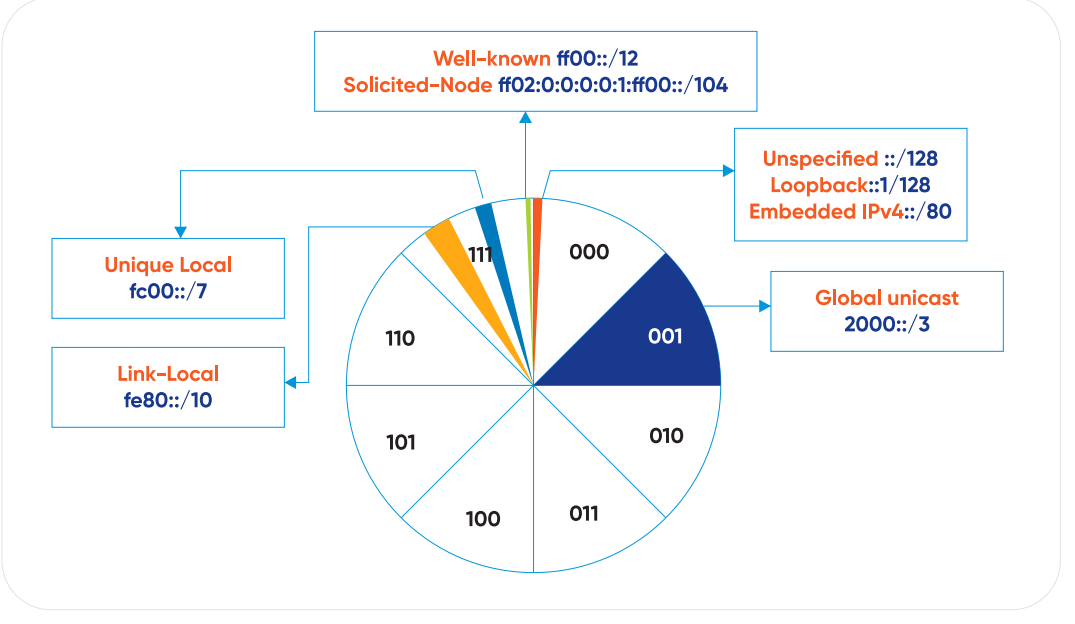


Hình 34. Chi tiết phân loại IPv6 theo cách thức và phạm vi hoạt động

Trong sơ đồ này mỗi loại địa chỉ đều có cách biểu diễn riêng, điều này do tổ chức IANA (Assigned Numbers Authority) quy định.

Nhắc lại:
- Địa chỉ Anycast là một loại địa chỉ Unicast được khai báo chung cho nhiều cổng mạng nên không có cách phân loại riêng.
- Địa chỉ Broadcast cũng tương tự, không có định dạng riêng mà là một địa chỉ dành riêng thuộc Multicast.

Như đã trình bày trong chương 1, toàn bộ không gian địa chỉ IPv6 được chia thành tám phân vùng bằng nhau thông qua sử dụng ba bit đầu tiên. Phân vùng có ba bit đầu tiên 001 được dùng để phân bổ thực tế được gọi là Global Unicast Address.



Hình 35. Chi tiết các loại địa chỉ IPv6 theo các phân vùng

Các địa chỉ Unique Local Address (ULA), Link Local Unicast (LLU) thuộc phân vùng 111. Địa chỉ Multicast cũng thuộc phân vùng 111, trong khi đó chỉ có các địa chỉ Unicast đặc biệt là thuộc phân vùng 000.

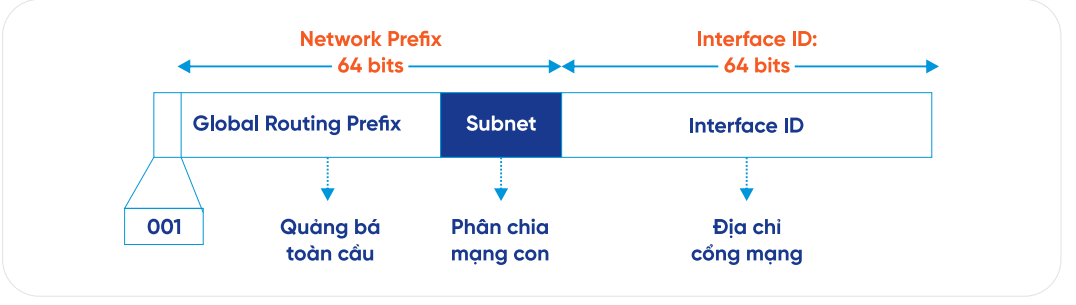
Như vậy phân vùng 001 là được dành riêng cho GUA, các phân vùng 000 và 111 được sử dụng một không gian rất ít, còn lại năm vùng còn trống để dành cho việc phát triển trong tương lai.

Nhắc lại:
- Vùng địa chỉ GUA 001 (/3) được chia thành 512 dãy địa chỉ /12. Từ năm 2006 đến nay mới được phân bổ 8 dãy /12, chưa đến 2% vùng 001 được phân bổ.

Nội dung tiếp theo sẽ phân tích đặc điểm chi tiết của từng loại địa chỉ.

3.4. ĐỊA CHỈ GLOBAL UNICAST ADDRESS (GUA)

Địa chỉ GUA được dùng phổ biến hơn so với địa chỉ Unique Local Address (ULA) bởi vì kỹ thuật NAT không được khuyến cáo đối với IPv6. Địa chỉ GUA hiện đang được phân bổ thuộc phân vùng có ba bit bắt đầu là 001. Với cách viết Hexa, địa chỉ GUA có dạng là 2000::/3 (viết tiếp 125 số 0 tiếp theo ba bit đầu, gom 4 bit đầu thành một số Hexa là 2). Thông thường kiến trúc chung của các địa chỉ Unicast gồm hai phần đều bằng 64 bit là: Network Prefix và Interface ID, riêng với GUA phần Network Prefix được chia thành hai phần con là: Global Routing Prefix và Subnet.



Hình 36. Cấu trúc của địa chỉ GUA được phân bổ thực tế

Global Routing Prefix:

Đây là phần địa chỉ đại diện cho một đơn vị tổ chức được quảng bá trên mạng toàn cầu Internet. Theo RFC 3177 số bit tối thiểu cho phần này là 48 bit hay còn gọi là /48. Như vậy trên mạng Internet sẽ không tồn tại những IPv6 Route từ /49 trở đi, điều này giống như quy định /24 tối thiểu đối với IPv4. Tùy theo quy mô của đơn vị, độ dài của phần Global Prefix sẽ khác nhau. Ví dụ như tại Việt Nam, các cơ quan, tổ chức khi đăng ký địa chỉ IPv6 với Trung tâm Internet Việt Nam (VNNIC) thường được phân bổ /48, riêng đối với các nhà mạng thì được cấp dãy /32.

Subnet:

Do phần Interface-ID được quy định có độ dài cố định 64 bit nên khoảng bit giữa Global Routing Prefix và Interface ID được dùng để các cơ quan, tổ chức đăng ký IPv6 phân chia mạng con cho đơn vị của mình. Mỗi đơn vị luôn có nhiều hơn một dãy mạng, ví dụ như có nhiều phân hệ, nhiều VLAN, nhiều vị trí kết nối... nên cần phân bổ nhiều dãy /64 cho các đơn vị đó. Chính vì thế số bit phần Subnet giúp các đơn vị thuận tiện phân chia mạng con thay vì phải mượn số bit ở phần Interface-ID như đối với IPv4.

Nếu Global Routing Prefix là 48 bit thì độ dài của Subnet sẽ là 16 bit. Trường hợp các đơn vị là khách hàng của nhà mạng thì dãy địa chỉ được nhà mạng cấp có thể là /60, /56... nên số bit dành cho phân chia mạng con sẽ ngắn lại.

Interface ID:

Những bit này đại diện cho một cổng thiết bị mạng hay máy tính hiện diện trên một phân đoạn mạng, giống như số nhà trên một con đường tạo nên địa chỉ nhà. Theo quy định của RFC 2373, những nơi nào có sự hiện diện của máy tính, ví dụ như một VLAN thì sẽ được phân một dãy mạng (Network Prefix) /64 (gồm Global Routing Prefix và Subnet), Interface ID của các máy tính trên mỗi phân đoạn mạng này là duy nhất. Với kỹ thuật SLAAC (Stateless Address Auto-Configuration), các thiết bị mạng có thể tự gán địa chỉ IPv6 cho chính mình thay vì sử dụng máy chủ DHCP Server, phần địa chỉ Interface ID được tạo ra tự động từ địa chỉ MAC (kỹ thuật EUI-64) hoặc ngẫu nhiên.

Chú ý:

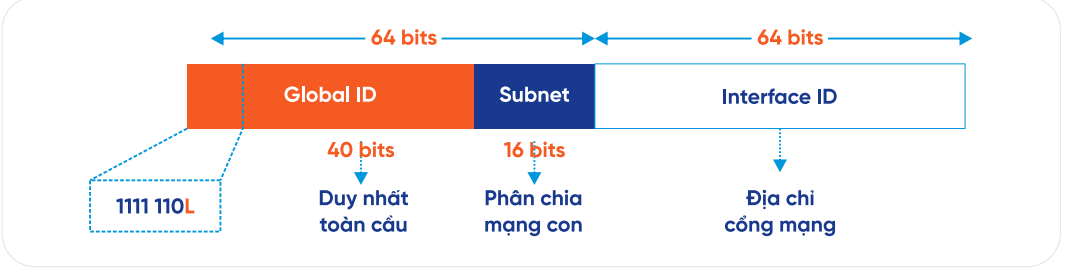
- Phần Network Prefix theo quy định là /64 nhưng trong thực tế người quản trị có thể khai báo giá trị khác như /65 cho đến /127. Với cách khai này các thiết bị vẫn có thể làm việc bình thường nhưng một số dịch vụ như SLAAC, NDP... không thể hoạt động, vì thế phải cần tuân theo quy định này.
- Một số trường hợp đặc biệt có thể sử dụng Network Prefix khác với /64 như địa chỉ Loopback, kết nối Poin-to-Point ... Những vấn đề này sẽ được trình bày sau.

3.5. ĐỊA CHỈ UNIQUE LOCAL ADDRESS (ULA)

Địa chỉ ULA tương ứng với địa chỉ IPv4 Private, phạm vi hoạt động chỉ trong các mạng nội bộ và không có ý nghĩa trên mạng Internet. Điều khác biệt quan trọng nhất giữa ULA và IPv4 Private là dù là địa chỉ nội bộ nhưng là duy nhất đối với mỗi hệ thống mạng. Việc này sẽ giúp các công ty dùng địa chỉ ULA nếu kết nối với nhau (ví dụ như qua VPN hoặc sáp nhập công ty) thì địa chỉ ULA của các công ty không trùng nhau nên không gây xung đột khi kết nối.

Chú ý:
- Để bảo đảm địa chỉ ULA là duy nhất cho mỗi hệ thống mạng thì không nên quy hoạch địa chỉ ULA thủ công mà nên dùng các công cụ tạo địa chỉ tự động. Có rất nhiều công cụ trực tuyến miễn phí trên Internet để tạo địa chỉ ULA tự động, từ khóa để tìm kiếm các công cụ này là: "Unique Local IPv6 Generator"

Địa chỉ ULA được mô tả trong RFC 4193 trong đó quy định 7 bit đầu tiên là "1111 110" nên địa chỉ đại diện của ULA là FC00::/7. Với quy định này, không gian địa chỉ của ULA rất lớn, trong thực tế bit số 8, có tên gọi là L (Local), được dùng để phân chia địa chỉ ULA thành hai phần, cụ thể như sau:



Hình 37. Cấu trúc của địa chỉ ULA

- Với L=0 địa chỉ ULA có dạng là FC00::/8, đây là dãy địa chỉ được dành riêng, dự phòng cho tương lai.
- Với L=1 địa chỉ ULA có dạng là FD00::/8, dãy địa chỉ này được phép sử dụng trong thực tế.

Như vậy với phần địa chỉ đại diện là FD00::/8 các công cụ tạo địa chỉ ULA tự động sẽ tạo ngẫu nhiên 48 bit nữa để cho ra dãy địa chỉ là /48, tương ứng với phần Subnet là 16 bit dùng để phân chia con cho hệ thống mạng nội bộ.

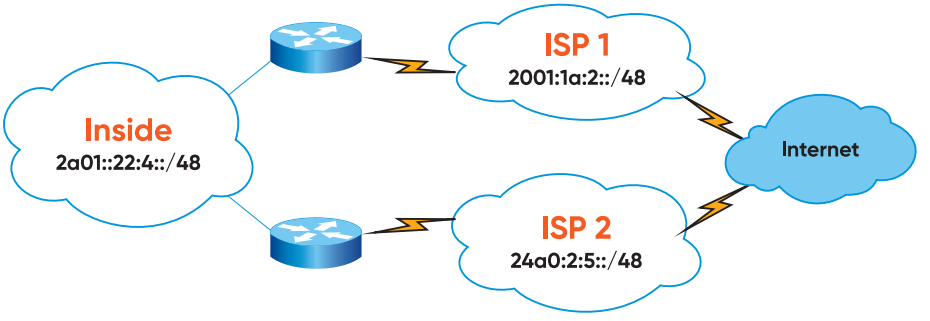
Chú ý:
- Trước đây cũng có một địa chỉ tương tự, chỉ có ý nghĩa cho mạng nội bộ, có tên là Site Local Address với địa chỉ đại diện là FEC0::/10 nhưng có nhiều vấn đề phát sinh nên được thay thế bằng địa chỉ ULA.

Địa chỉ ULA chỉ có nghĩa ở phạm vi nội bộ nên những hệ thống sử dụng địa chỉ này không thể truy cập được Internet vì thế cần khai địa chỉ GUA này song song với địa chỉ này hoặc sử dụng thêm cơ chế chuyển đổi địa chỉ IPv6. Hiện nay tổ chức IETF không khuyến cáo sử dụng cơ chế chuyển đổi địa chỉ NAT (Network Address Translation) như đối với IPv4 nhưng trước nhu cầu sử dụng như trường hợp dùng địa chỉ ULA thì IETF đã đưa ra RFC 6296 (6/2011) giới thiệu kỹ thuật NPTv6 (IPv6-to-IPv6 Network Prefix Translation). Khác với NAT cho phép chuyển đổi một địa chỉ IPv4 sang một địa chỉ IPv4 khác và lưu thông tin (vào NAT Table) thì NPTv6 chỉ cho phép chuyển đổi IPv6 Prefix này sang IPv6 Prefix khác và không cần lưu thông tin.

Chú ý:
- NAT được gọi là cơ chế Stateful vì phải lưu thông tin chuyển đổi cho từng địa chỉ còn NPTv6 là cơ chế Stateless vì chỉ chuyển đổi phần Prefix, giữ nguyên phần còn lại nên không cần lưu thông tin.

RFC 7296 này không được phê duyệt chính thức mà vẫn được xếp vào loại thử nghiệm (Experimental). Dù vậy nhiều hãng đã cung cấp tính năng này trên thiết bị của mình. NPTv6 là một kỹ thuật mang lại rất nhiều lợi ích trong thực tế, vì thế cần xem xét lựa chọn tính năng này khi mua sắm các thiết bị định tuyến hay tường lửa.

Nguyên lý hoạt động của NPTv6 là khi một bản tin IPv6 đi qua thiết bị hỗ trợ NPTv6 thì phần Prefix của địa chỉ nguồn (Source IPv6) sẽ được thay thế bởi một Prefix khác. Phần Prefix này được người quản trị quy hoạch và khai báo. Chỉ có Prefix thay đổi và phần còn lại của địa chỉ IPv6 được giữ nguyên nên thiết bị hỗ trợ NPTv6 không cần phải lưu thông tin chuyển đổi cho mỗi phiên kết nối.



Hình 38. Mô hình hoạt động với NPTv6

Với nguyên tắc hoạt động này, kỹ thuật NPTv6 mang lại rất nhiều lợi ích khi được áp dụng thực tế:

Dự phòng kết nối (Failover): Trong trường hợp hệ thống có kết nối đa hướng, việc áp dụng NPTv6 nhiều hướng giúp khi một kết nối bị sự cố thì hệ thống vẫn có thể truy cập qua kết nối còn lại, bảo đảm dự phòng kết nối cho hệ thống.

Phân chia tải (Load-sharing): Kết nối từ bên trong ra bên ngoài có thể được phân tán qua cách hướng kết nối khác nhau, mỗi hướng được chuyển đổi sang Prefix của mỗi nhà mạng.

Định tuyến đối xứng (Symmetric Routing): Khi một kết nối ra ngoài đi qua một nhà mạng thì kết quả trả về sẽ đi qua lại đúng hướng cũ, có nghĩa hướng đi và về của một kết nối là như nhau, không thay đổi. Việc này giúp dễ kiểm soát hướng đi về của các bản tin, độ trễ hướng đi và về gần như nhau và tránh bị sự cố khi qua một số tường lửa kiểm soát chặt (Stateful Firewall).

Không phụ thuộc nhà mạng: Khi thay đổi sang nhà mạng khác thì địa chỉ bên trong không cần phải thay đổi theo mà chỉ cần khai báo lại Prefix cho NPTv6. Đặc biệt, tính năng này rất phù hợp với các hệ thống sử dụng địa chỉ ULA. Các địa chỉ ULA nội bộ sẽ được chuyển đổi Prefix sang Prefix GUA do nhà mạng cung cấp.

Dù mang lại nhiều lợi ích thực tế nhưng NPTv6 vẫn lặp lại những hạn chế của NAT như không thể cung cấp kết nối End-to-End, mã hóa IPSec vẫn không thể được, một số dịch vụ không thể hoạt động ...

Với kiểu chuyển đổi từ địa chỉ IPv6 này sang địa chỉ IPv6 khác, hay còn gọi là NAT66 thì IETF hoàn toàn không khuyến cáo vì kỹ thuật NAT trước đây được sinh ra nhằm giúp làm chậm sự cạn kiệt địa chỉ IPv4 trong khi IPv6 ra đời để giải quyết sự cạn kiệt của IPv4 nên NAT bị loại bỏ đối với IPv6. Trong thực tế, nhiều người dùng vẫn mong muốn sử dụng NAT66 để che dấu địa chỉ thực sự ở bên trong, hy vọng giúp tăng bảo mật hoặc thuận tiện trong việc phân tán tải trong trường hợp kết nối dự phòng với nhiều nhà mạng hoặc không cần phải thay đổi địa chỉ mạng bên trong khi thay đổi nhà mạng. Vì thế, dù IETF không khuyến cáo nhưng nhiều nhà mạng cũng đã tích hợp tính năng NAT66 vào trong thiết bị của mình.

Chú ý: **Danh sách thiết bị hỗ trợ tính năng NAT66:**

- Fortinet FortiGate firewall hỗ trợ NAT66, NAT64 và NAT46.
- Cisco ASA firewall hỗ trợ NAT66
- Juniper Junos router hỗ trợ NAT66.
- Juniper SRX firewall hỗ trợ source NAT66.
- F5 BIG-IP hỗ trợ NAT66.
- Check Point firewalls từ phiên bản R76 hỗ trợ NAT66.
- Hệ điều hành nhúng OpenWrt hỗ trợ NAT66.
- H3C SecPath Firewall hỗ trợ NAT66.
- SonicWall hỗ trợ NAT66.

Khi cần trang thiết bị mạng mới, cần cân nhắc nhu cầu sử dụng tính năng NAT66 để lựa chọn cho phù hợp.

3.6. ĐỊA CHỈ LINK LOCAL ADDRESS (LLA)

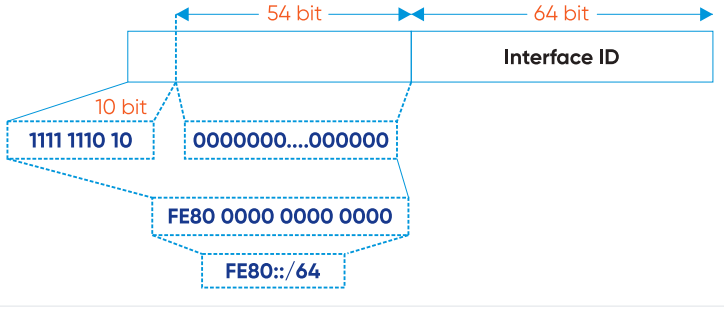
Đây là loại địa chỉ mới, không có địa chỉ IPv4 tương đương. Điểm khác biệt của LLA so với các địa chỉ khác là phạm vi hoạt động của nó chỉ trong một phân đoạn mạng (như một VLAN) hay trên một cổng giao diện của Router. Các bản tin có địa chỉ đích là LLA chỉ hoạt động trên một phân đoạn mạng, không được Router chuyển tiếp sang các cổng giao diện khác như đối với địa chỉ GUA hay ULA. Những đặc điểm đáng chú ý của LLA như sau:

- Tất cả các cổng giao diện chạy IPv6 đều phải có địa chỉ này.
- LLA thường được tạo tự động và cũng có thể khai báo thủ công.
- Khác với GUA và ULA, mỗi cổng giao diện của Router chỉ có một địa chỉ LLA duy nhất.
- LLA là duy nhất trên mỗi phân đoạn mạng nhưng có thể trùng nhau ở phân đoạn mạng khác.

Chú ý:

- Mục đích của địa chỉ LLA là giúp tất cả các cổng giao diện IPv6 đều có một địa chỉ mạng để trao đổi thông tin cho nhau thay vì sử dụng địa chỉ MAC như đối với IPv4. LLA được dùng để xác định các Neighbor trên cùng một phân đoạn mạng và để trao đổi với DHCP Server để nhận địa chỉ GUA hoặc ULA.
- Có một dãy địa chỉ có chức năng khá giống ở IPv4 là địa chỉ APIPA (Automatic Private IP Addressing) 169.254.0.0/16 nhưng mục đích và cách thức hoạt động khác so với LLA.

Theo quy định trong RFC 4291 địa chỉ LLA có 10 bit đầu tiên là **1111 1110 10**, 54 bit tiếp sau đó không quy định nhưng thường là giá trị 0 nên địa chỉ đại diện của LLA là **FE80::/10**.



Hình 39. Cấu trúc của địa chỉ LLA

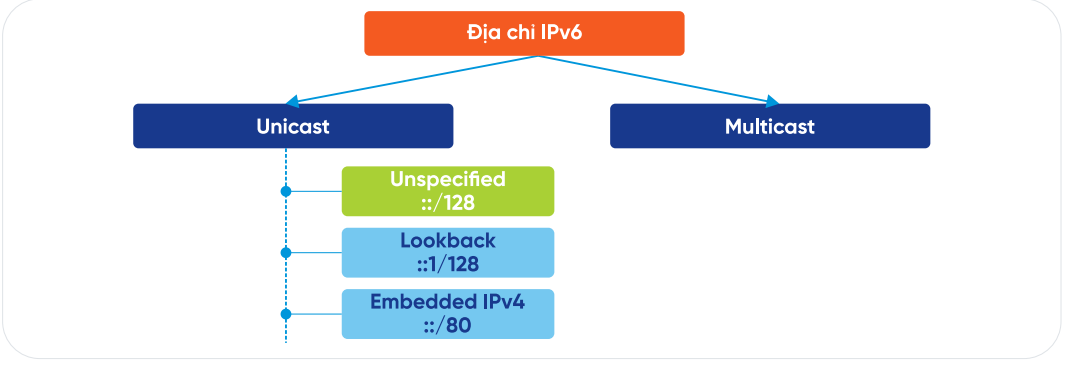
Chú ý:

- Dù không ai quy định 54 bit tiếp theo là những số 0 nên bạn có thể đặt giá trị khác nhưng một số ứng dụng hoặc thiết bị sẽ không chấp nhận những giá trị này, vì vậy tốt nhất nên giữ nguyên 54 bit giá trị 0. Do đó địa chỉ LLA trong thực tế thường có dạng FE80::/64 nên có thể trùng nhau nếu ở các phân đoạn mạng khác nhau.

3.7. ĐỊA CHỈ UNSPECIFIED

Địa chỉ **Unspecified** trong IPv6, với toàn bộ 128 bit đều bằng 0, được biểu diễn dưới dạng **::/128**, tương ứng với địa chỉ **0.0.0.0/32** trong IPv4. Địa chỉ này không được gán cho bất kỳ giao diện (Interface) nào và không thể sử dụng làm địa chỉ đích cho bất kỳ gói tin nào. Trong trường hợp một giao diện chưa được cấu hình địa chỉ IPv6, các gói tin gửi đi từ giao diện đó sẽ không có địa chỉ nguồn. Khi đó, địa chỉ **Unspecified ::/128** được sử dụng làm đại diện.

Ví dụ, khi bạn cấu hình địa chỉ tĩnh cho một giao diện hoặc nhận địa chỉ động từ DHCP, địa chỉ này cần trải qua quá trình **Kiểm tra trùng lặp địa chỉ (Duplicate Address Detection – DAD)** trước khi được sử dụng. Trong quá trình này, các gói tin kiểm tra trùng lặp sẽ sử dụng **::/128** làm địa chỉ nguồn, đảm bảo tính chính xác và hợp lệ trong việc gán địa chỉ.

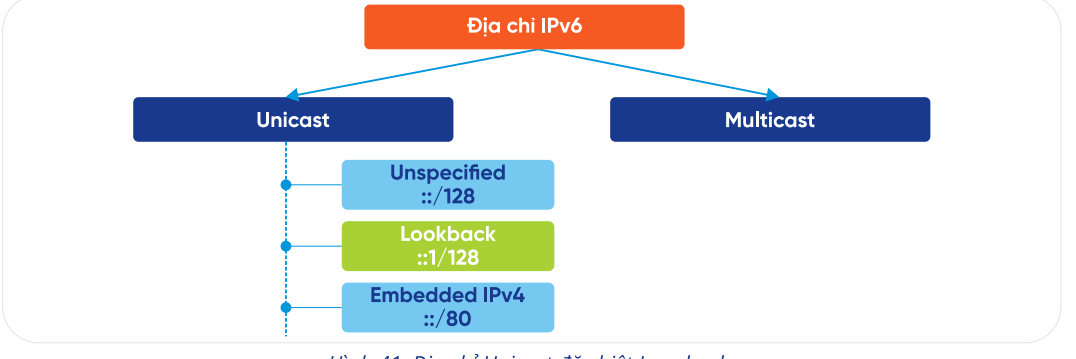


Hình 40. Địa chỉ Unicast đặc biệt Unspecified

3.8. ĐỊA CHỈ LOOPBACK

Địa chỉ **Loopback** trong IPv6, được biểu diễn là **::1/128**, tương tự với địa chỉ Loopback trong IPv4 (127.0.0.0/8). Đây là địa chỉ đại diện cho một giao diện mạng ảo trên thiết bị, cho phép gửi gói tin mà không cần rời khỏi thiết bị, thay vào đó gói tin sẽ được phản hồi lại ngay lập tức. Ví dụ, khi sử dụng lệnh **PING** tới địa chỉ Loopback, thiết bị tự kiểm tra hoạt động của bộ giao thức TCP/IP hoặc xác nhận khả năng truy cập các ứng dụng (như web) trên chính thiết bị đó.

Khác với IPv4, vốn dành một dải địa chỉ lớn (127.0.0.0/8, tương đương hơn 16 triệu địa chỉ) cho mục đích Loopback, IPv6 tối ưu hóa bằng cách chỉ sử dụng một địa chỉ duy nhất **::1/128**, trong đó chỉ bit cuối cùng có giá trị 1. Thiết kế này giúp đơn giản hóa và tiết kiệm tài nguyên, phù hợp với mục tiêu tinh gọn của IPv6.



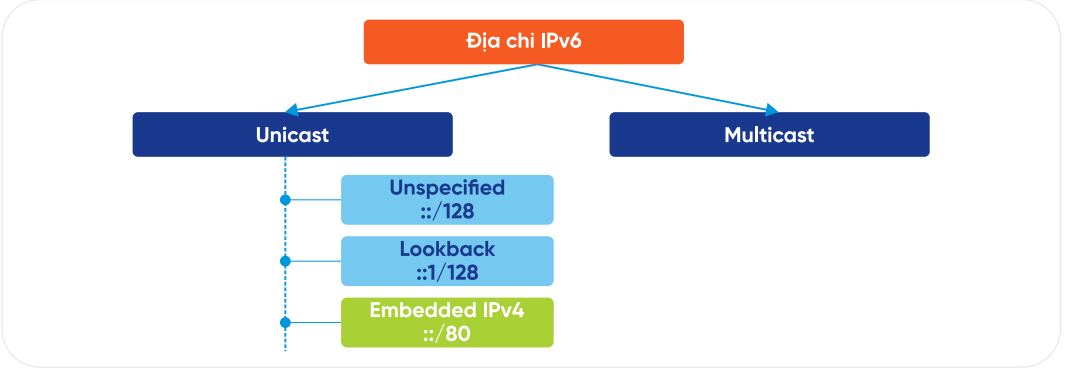
Hình 41. Địa chỉ Unicast đặc biệt Loopback

Chú ý:

- Địa chỉ LocalHost: Khi cần kiểm tra dịch vụ trên một máy chủ web bạn có thể truy cập thông qua địa chỉ Loopback **http://127.0.0.1** hoặc theo cách khác là **http://localhost**. Như vậy tên gọi LocalHost như là tên miền (Domain name) cục bộ thay cho địa chỉ Loopback.
- Loopback Interface: Đây là một Interface ảo trên các thiết bị mạng hay máy tính, có vai trò như các Interface vật lý. Có thể gán địa chỉ Unicast (IPv4 Private/Public, IPv6 Global Unicast/Unique Local) cho các Loopback Interface và từ bên ngoài có kết nối đến các địa chỉ này (như khai báo Routing, PING, giám sát thiết bị ...) không như với địa chỉ Loopback.

3.9. ĐỊA CHỈ IPv4 EMBEDED

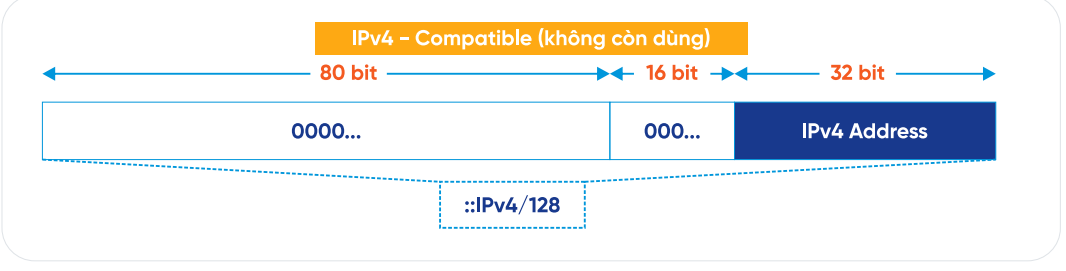
Có nhiều giải pháp để chuyển đổi sang IPv6 và một trong những số đó là sử dụng đường hầm (Tunnel) IPv4 để kết nối các hệ thống IPv6 với nhau. Các địa chỉ IPv4 tạo nên đường hầm sẽ được "nhúng" vào trong một cấu trúc để tạo thành địa chỉ IPv6, phục vụ cho việc định tuyến các bản tin IPv6 qua đường hầm này. Đây chính là cơ chế của IPv4 Embeded và có hai quy định cho địa chỉ này.



Hình 42. Địa chỉ Unicast đặc biệt IP4-Embeded

IPv4-compatible IPv6 (đã không còn sử dụng – Deprecated)

Cấu trúc gồm 96 bit 0 kết hợp với 32 bit địa chỉ của IPv4 tạo thành một địa chỉ IPv6 có dạng **::IPv4/64.**

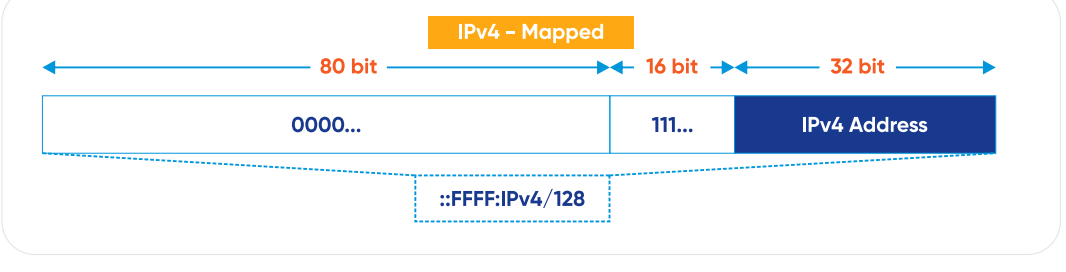


Hình 43. Địa chỉ Unicast đặc biệt IPv4-compatible không còn được sử dụng

Địa chỉ này được đề xuất nhằm nhanh chóng triển khai IPv6 dựa trên nền tảng IPv4 nhưng cách thức triển khai theo giải pháp này khá phức tạp và địa chỉ IPv4 bắt buộc phải là địa chỉ công cộng (Public Address) nên đã không được áp dụng nhiều trong thực tế và đã bị đề nghị ngưng sử dụng.

IPv4-mapped IPv6

Địa chỉ này cũng tương tự IPv4-compatible nhưng cấu trúc gồm 80 bit 0 ở vị trí đầu tiên, tiếp theo sau là 16 bit 1 kết hợp với 32 bit địa chỉ của IPv4 tạo thành địa chỉ IPv6 có dạng **::FFFF:IPv4/64.**



Hình 44. Cấu trúc địa chỉ IPv6 đặc biệt IP4-Mapped

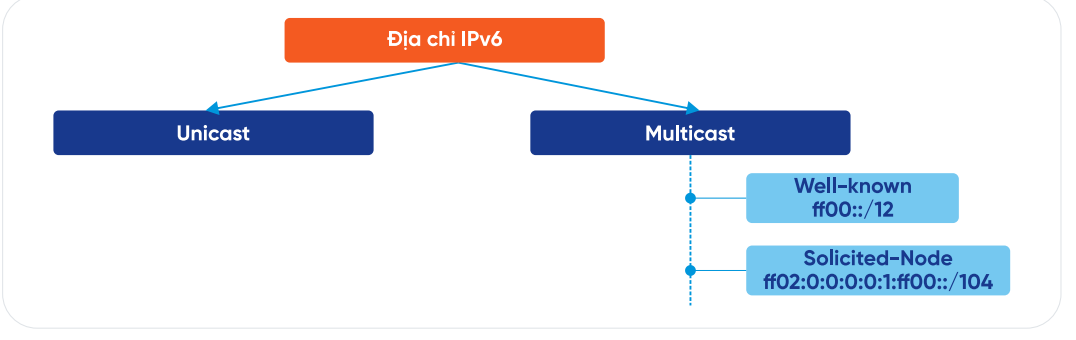
Địa chỉ này được dùng trong thực tế thay thế cho IPv4-compatible IPv6. Một ví dụ điển hình là trong triển khai chuyển đổi mạng MPLS sang IPv6.

Chú ý:
- Một số giải pháp Tunnel về sau đã phát sinh ra các dạng địa chỉ IPv4-Embeded khác, ví dụ như kỹ thuật **6to4**. Tiền tố (Prefix) 2002::/16 kết hợp với địa chỉ IPv4 /32 tạo thành dãy địa chỉ IPv6 /48 để quy hoạch cho hệ thống và bảo đảm thiết lập Tunnel tự động thông qua các địa chỉ IPv4 kết hợp.
- Giải pháp **6RD** (thay thế cho 6to4) lại sử dụng một dãy địa chỉ khác được cấp phát (là /32) để kết hợp với địa chỉ IPv4, tạo thành địa chỉ IPv6 thay vì dùng Prefix 2002::/16.

3.10. ĐỊA CHỈ MULTICAST

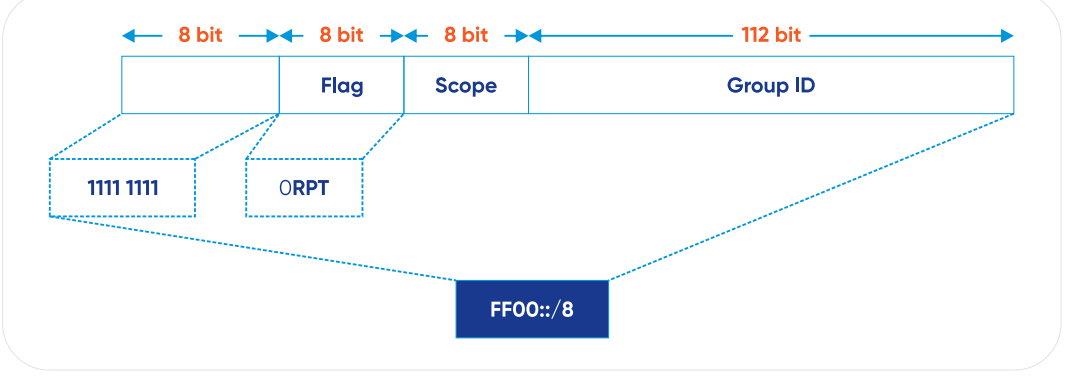
Multicast là thành phần thứ hai trong cách phân loại địa chỉ IPv6 theo đặc điểm (Type). Multicast trong IPv6 có cách thức hoạt động khá giống như đối với IPv4 nhưng về thiết kế thì có thêm nhiều tính năng và tối ưu hơn, ví dụ như: Multicast được chia ra Scope hoặc có thêm địa chỉ mới rất đặc biệt là Solicited Node.

Chú ý:
- Địa chỉ Multicast chỉ có thể là địa chỉ đích chứ không thể làm địa chỉ nguồn của các bản tin.



Hình 45. Thành phần của địa chỉ IPv6 Muticast

Theo quy định, 8 bit đầu tiên của địa chỉ Multicast đều là 1 nên dạng biểu diễn của địa chỉ này là FF00::/8, tương ứng 224.0.0.0/4 của IPv4. Phần tiếp theo 8 bit đầu tiên trong cấu trúc của Multicast là 4 bit Flag (tính năng), 4 bit Scope (phạm vi) và 112 bit còn lại được dùng để định danh nhóm Multicast (Group ID).



Hình 46. Cấu trúc của địa chỉ Multicast

Flag là một trong những cải tiến của địa chỉ IPv6 Multicast, các vị trí bit của Flag có đặc điểm sau:

- Bit 0 đầu tiên được sử dụng thực tế còn bit 1 đang để dự phòng.
- Bit R (Ren-dezvous Point) bằng 1 nếu định tuyến Multicast được sử dụng (RFC 3956).
- Bit P (Network Prefix) được bật nếu địa chỉ Multicast có chứa Unicast Prefix (RFC 3306).
- Bit T (Transient) dùng để phân biệt địa chỉ Multicast này do tổ chức IANA quy định (T=0) hay do người dùng tự định nghĩa (T=1) cho ứng dụng của mình (trường hợp ứng dụng đó cần sử dụng Multicast, RFC 4291).

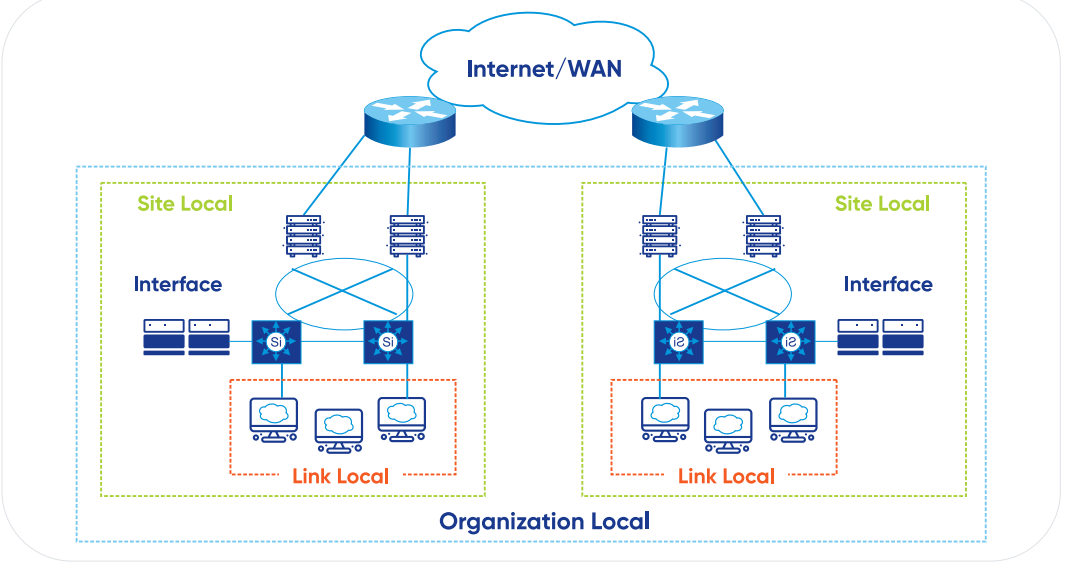
Ở đây chỉ giới thiệu tổng quan về địa chỉ Multicast chứ không đi sâu và trình bày chi tiết.

Scope cũng là thành phần được cải tiến nhằm phân chia phạm vi hoạt động địa chỉ IPv6, tương đối giống như của IPv6 Unicast (được chia thành các phạm vi Global Unicast, Unique Local và Link Local như đã trình bày). Quy định phạm vi của các bit thuộc Scope như sau:

Mã Scope	Tên
0	Để dành
1	Mức Interface-local
2	Mức Link-local
3	Để dành
4	Admin-local
5	Site-local
6, 7	Chưa quy định
8	Mức Organization-local
9, A, B, C, D	Chưa quy định
E	Mức Global
F	Để dành

Bảng 4. Danh sách Scope của IPv6 Multicast

Hình dưới mô tả cho ý tưởng của phạm vi hoạt động của địa chỉ IPv6 Multicast. Dù vậy, hiện nay chủ yếu phạm vi Link-Local được dùng trong thực tế, các phạm vi khác sẽ được ứng dụng trong tương lai.

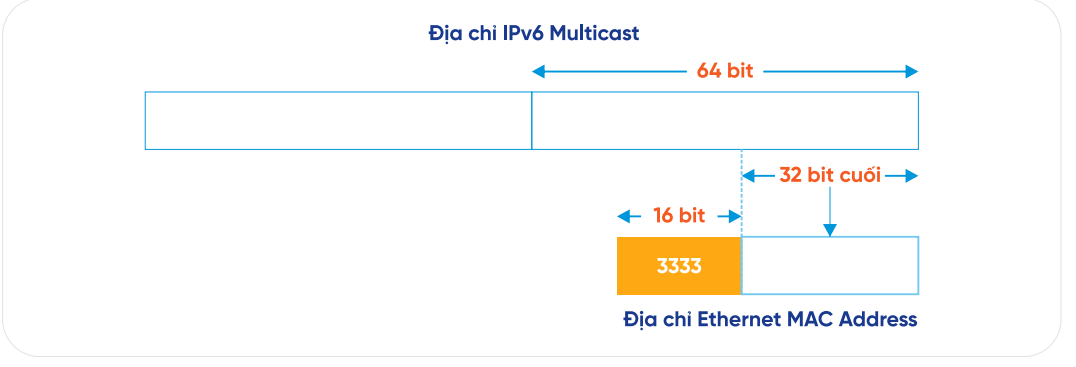


Hình 47. Minh họa Scope của địa chỉ Multicast

Do 8 bit đầu tiên bằng 1 tương ứng với giá trị Hexa FF, tiếp theo là 4 bit Flag và 4 bit của Scope, nếu không tính các bit Flag thì vị trí của Scope sẽ là vị trí X trong cách biểu diễn FF0X::/16. Theo bảng quy định trên thì X=1,2,4,5,8,E. Một số ví dụ về phạm vi của địa chỉ IPv6 Multicast:

- **FF02::2** đại diện cho tất cả các Router trên cùng Link
- **FF05::2** đại diện cho tất cả các Router trên cùng một Site

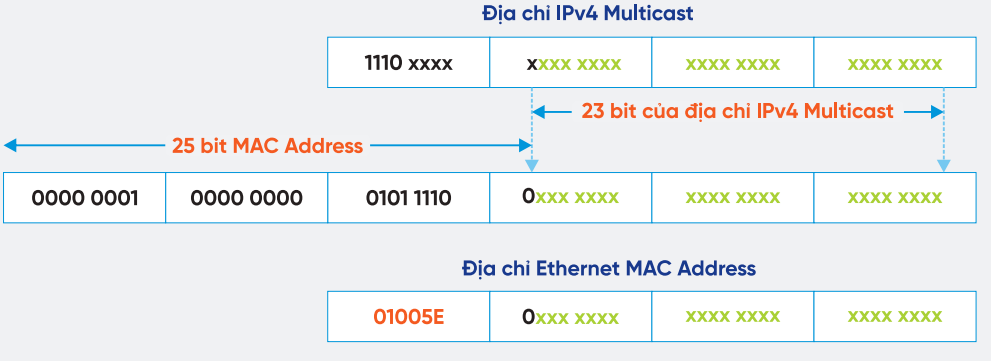
Cũng như IPv4, địa chỉ IPv6 Multicast cũng được đóng vào khung Ethernet theo quy định riêng để giúp các Interface khi nhận được khung tin dễ dàng nhận biết khung tin đó thuộc nhóm Multicast mà Interface đó tham gia hay không, nếu không thì lọc bỏ khung tin.



Hình 48. Ethernet Frame của bản tin IPv6 Multicast

Cách thức ánh xạ địa chỉ IPv6 Multicast được thực hiện bằng cách sử dụng 16 bit có dạng Hexa là 3333 kết hợp với 32 bit cuối cùng địa chỉ Multicast.

Chú ý: • Nhắc lại cách thức truyền bản tin IPv4 Multicast vào khung Ethernet như hình dưới, cách ánh xạ của IPv6 Multicast cũng tương tự như IPv4 nhưng khác số bit và tiền tố.



Hình 49. Ethernet Frame của bản tin IPv4 Multicast

3.11. ĐỊA CHỈ WELL-KNOWN MULTICAST

Phần trên đây là quy định chung về cấu trúc của địa chỉ IPv6 Multicast, từ quy định này tổ chức IANA đã quy định cụ thể một số địa chỉ để ứng dụng trong thực tế. Các địa chỉ này được giới thiệu ban đầu trong RFC 2375, RFC 3307, RFC 4291. Hiện nay danh sách chi tiết và được cập nhật mới nhất là tại trang web của IANA: **https://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml.**

Dưới đây là danh sách một số địa chỉ quy định và phạm vi của mỗi địa chỉ.

PHẠM VI	ĐỊA CHỈ	MÔ TẢ
Interface-local	ff01::1	All-nodes address
	ff01::2	All-routers address
	ff01::fb	mDNSv6
Link-local	ff02::1	All nodes
	ff02::2	All routers
	ff02::4	DVMRP routers
	ff02::5	OSPFv3 All SPF routers
	ff02::6	OSPFv3 All DR routers
	ff02::7	ST routers
	ff02::8	IS-IS for IPv6 routers
	ff02::9	RIP routers
	ff02::a	EIGRP routers
	ff02::d	PIM routers
	ff02::12	VRRP version 3
	ff02::16	MLDv2 reports[24]
	ff02::1:2	DHCPv6 servers
	ff02::1:3	All LLMNR hosts
Site-local	ff05::1:3	All DHCPv6 servers
	ff05::2	All-routers address
	ff05::fb	mDNSv6
Không phụ thuộc phạm vi	ff0x::c	Simple Service Discovery Protocol
	ff0x::fb	Multicast DNS
	ff0x::101	Network Time Protocol
	ff0x::108	Network Information Service
	ff0x::181	Precision Time Protocol (PTP) version 2 messages (Sync, Announce, etc.) except peer delay measurement
	ff02::6b	Precision Time Protocol (PTP) version 2 peer delay measurement messages
	ff0x::114	Used for experiments

Bảng 5. Danh sách địa chỉ Well-known Multicast

Thường mỗi địa chỉ được gán cho một chức năng và thuộc một phạm vi nhưng có một số địa chỉ cùng chức năng nhưng ở phạm vi khác nhau, ví dụ như địa chỉ Multicast dành cho DHCP, All-Router ... Ngoài ra còn có loại địa chỉ cố định (Permanent) và có thể hoạt động ở tất cả các Scope, dù ở Scope nào thì phần địa chỉ nhóm (Multicast group ID) đều không thay đổi. Các địa chỉ này được biểu diễn có ký tự X trong địa chỉ.

Tùy theo chức năng, mỗi Interface có thể tham gia nhiều nhóm Multicast khác nhau nên khi kiểm tra trạng thái của một số Interface sẽ thấy rất nhiều nhóm trên Interface.

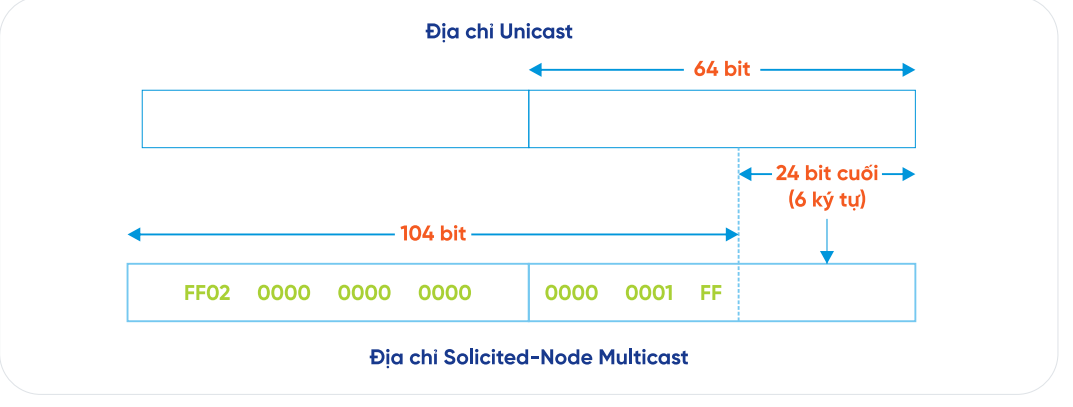
Địa chỉ **ff02::1** đại diện cho tất cả các node mạng trên một phân đoạn mạng (phạm vi Link) nên có ý nghĩa giống như địa chỉ Broadcast của IPv4. Như vậy một địa chỉ Multicast đặc biệt hoạt động thay thế cho địa chỉ Broadcast nên địa chỉ Broadcast không còn được dùng trong IPv6.

3.12. ĐỊA CHỈ SOLICITED-NODE MULTICAST

Địa chỉ **Solicited-Node Multicast** là một loại địa chỉ Multicast quan trọng và được sử dụng rộng rãi trong IPv6, hỗ trợ nhiều dịch vụ mạng phổ biến. Địa chỉ này được tạo tự động từ địa chỉ **Unicast** của một giao diện (Interface). Cụ thể, mỗi khi một giao diện được gán một địa chỉ Unicast, chẳng hạn như **Link Local, Unique Local** hoặc **Global Unicast**, một địa chỉ **Solicited-Node Multicast** tương ứng sẽ tự động được sinh ra và gán cho giao diện đó, đảm bảo khả năng giao tiếp hiệu quả trong mạng.

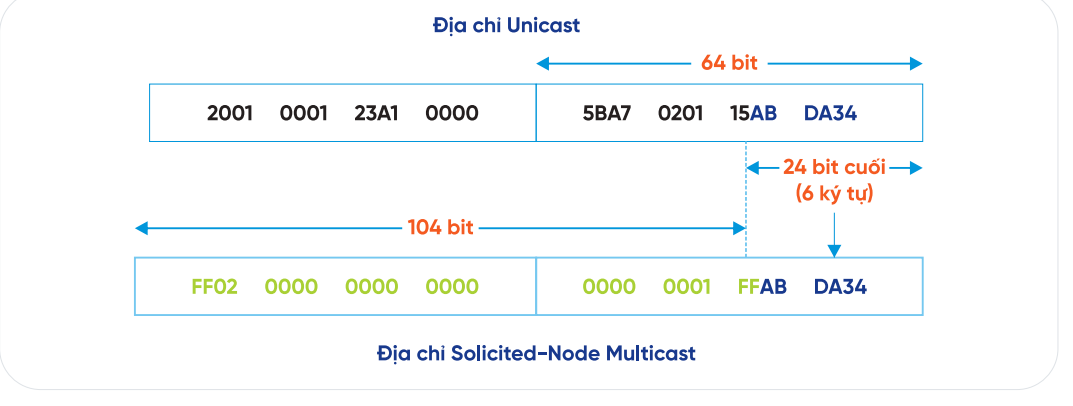
Chú ý:
- Một Interface có thể được gán nhiều địa chỉ Unicast nên Interface đó sẽ tham gia nhiều nhóm Solicited-Node Multicast tương ứng với từng địa chỉ Unicast.
- Tất cả các Interface IPv6 đều có địa chỉ Link Local nên chúng đều tham gia ít nhất một Solicited Node Multicast.

Địa chỉ Solicited-Node Multicast được tạo ra từ địa chỉ Unicast theo quy định như sau:



Hình 50. Nguyên tắc tạo Solicited-Node Multicast từ Unicast

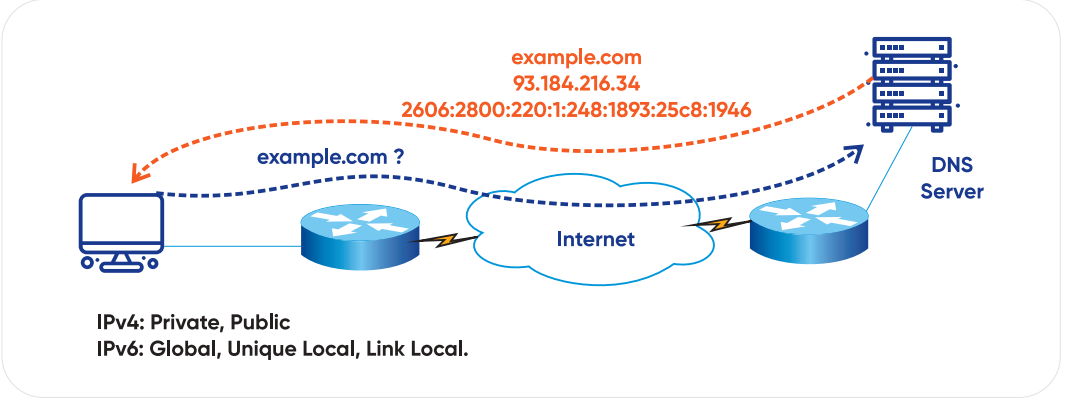
Lấy 24 bit cuối cùng của địa chỉ Unicast kết hợp với tiền tố **ff02:0:0:0:0:1:ff00::/104** (thường viết gọn **ff02::1:ff00/104**) để tạo thành địa chỉ Solicited-Node Multicast 128 bit.



Hình 51. Ví dụ nguyên tắc tạo Solicited-Node Multicast từ Unicast

3.13. QUY TẮC LỰA CHỌN ĐỊA CHỈ IPv6

IPv6 cho phép một Interface có thể được khai báo nhiều địa chỉ cùng lúc và chúng có vai trò như nhau (không giống vai trò địa chỉ Primary và Secondary như IPv4). Một Interface có thể có tất cả các loại địa chỉ IPv6 như Link Local, Unique Local và Global Unicast, cũng có thể có nhiều địa chỉ Global Unicast cùng lúc. Trong trường hợp sử dụng song song IPv4 và IPv6 (Dual Stack) thì Interface có thêm địa chỉ IPv4 bên cạnh các địa chỉ IPv6.



Hình 52. Minh họa truy cập Internet ở chế độ Dual Stack

Trong hình minh họa trên một máy tính, có cả địa chỉ IPv4 và các địa chỉ IPv6, truy vấn một tên miền và được DNS phản hồi lại cả địa chỉ IPv4 và IPv6 thì việc máy tính lựa chọn địa chỉ nào để tạo phiên kết nối là một vấn đề. Nếu địa chỉ IPv4 đang sử dụng là Private thì kết nối dùng địa chỉ IPv4 sẽ bị lỗi. Nếu địa chỉ IPv6 đang dùng là Unique Local thì kết nối bằng IPv6 cũng không thể được.

Ngoài các loại địa chỉ IPv6 như đã trình bày ở trên còn có một số loại địa chỉ IPv6 khác như:

Theo RFC 4941

Để tăng cường bảo mật, có hai địa chỉ Global Unicast được gán cho một Interface là "Public address" và "Temporary address". Temporary addresses là địa chỉ tạm phục vụ cho kết nối ra bên ngoài và sẽ thay đổi sau một thời gian ngắn còn Public address thường phục vụ cho kết nối hướng vào.

Theo RFC 4682

Mỗi địa chỉ IPv6 được gán động sẽ có một thời gian hoạt động nhất định gọi là Preferred, sau thời gian này địa chỉ đó trở thành Deprecated và một địa chỉ Preferred khác được sinh ra. Địa chỉ Deprecated sẽ tiếp tục được dùng nếu vẫn tồn tại kết nối đang sử dụng địa chỉ này, các kết nối mới không dùng địa chỉ Deprecated mà dùng địa chỉ Preferred mới. Địa chỉ Deprecated sẽ bị xóa sau thời gian Valid quy định (dù vẫn còn kết nối nếu có). Vậy tại một thời điểm có thể có cả hai địa chỉ IPv6 là Preferred và Deprecated.

Theo RFC 6275

IPv6 cho phép các máy tính chuyển vùng (Roaming) sang hệ thống mạng khác nhưng vẫn giữ kết nối như bình thường, giống như vẫn đang ở hệ thống mạng cũ. Để thực hiện điều này thì máy tính đó sẽ tạo kết nối giữa địa chỉ Home Address ở mạng cũ với địa chỉ Care-of Address ở mạng mới. Tính năng này không được sử dụng phổ biến trong thực tế nhưng chúng ta vẫn cần xét đến hai địa chỉ Home Address và Care-of Address trong quy tắc lựa chọn địa chỉ nguồn IPv6.

Như vậy có rất nhiều loại địa chỉ IPv6 để lựa chọn cho việc kết nối trong trường hợp Interface có nhiều địa chỉ. Mỗi hệ điều hành hoặc mỗi nhà cung cấp có thể có cơ chế chọn địa chỉ riêng nên để quy định, quy tắc chung RFC 6724 đã đề ra một quy trình lựa chọn gồm có các quy tắc cụ thể. Dù đây là quy tắc chung nhưng các ứng dụng triển khai thực tế có thể thay đổi thứ tự ưu tiên nếu cần. Các quy tắc lựa chọn địa chỉ nguồn cho kết nối cũng có thể áp dụng cho việc lựa chọn địa chỉ đích cho kết nối (trường hợp một thiết bị nhận được một bản tin có địa chỉ đích là Multicast thì địa chỉ cần phản hồi cũng cần phải lựa chọn tương ứng với địa chỉ nguồn của bản tin gửi đến). Việc lựa chọn địa chỉ nguồn sẽ phụ thuộc vào địa chỉ đích của kết nối cần thực hiện, sau đây là 8 quy tắc cho việc lựa chọn địa chỉ nguồn tương ứng với địa chỉ đích:

Quy tắc 1 (Prefer same address):

Nếu địa chỉ nguồn trùng địa chỉ đích thì địa chỉ nguồn đó được lựa chọn. Quy tắc này được sử dụng trong trường hợp một node mạng thực hiện kết nối với chính mình như dùng lệnh Ping tới địa chỉ của Interface hoặc kết nối web đến địa chỉ của Interface trên node mạng đó thì địa chỉ nguồn được sử dụng cho bản tin cũng chính là địa chỉ đích.

Quy tắc 2 (Prefer appropriate scope):

Ưu tiên chọn địa chỉ nguồn nào có phạm vi (Scope) gần giống với địa chỉ đích nhất. Địa chỉ IPv4 không có khái niệm Scope nên những địa chỉ IPv4 chuyển đổi sang IPv6 (như IPv4-mapped hoặc IPv4-compatible) sẽ được xem xét Scope như sau: dãy địa chỉ 169.254.0.0/16 được xem là Link-Local còn các địa chỉ IPv4 khác kể cả IPv4 Private (RFC 1918, 6598) được xem Global Unicast khi chuyển qua IPv6.

Quy tắc 3 (Avoid deprecated addresses):

Như trình bày, địa chỉ IPv6 chỉ có hiệu lực trong một khoảng thời gian được gọi là Preferred, sau khoảng thời gian này địa chỉ IPv6 được gọi là Deprecated. Quy tắc này chỉ định sử dụng địa chỉ Preferred làm địa chỉ nguồn để khởi tạo một kết nối mới.

Quy tắc 4 (Prefer home addresses):

Quy tắc này áp dụng trong trường hợp chuyển vùng (Roaming) như đã trình bày. Nếu một node mạng có cả địa chỉ Home Address và Care-of Address thì địa chỉ Home Address được ưu tiên sử dụng làm địa chỉ nguồn.

Quy tắc 5 (Prefer outgoing interface):

Có thể có nhiều Interface được dùng để gửi bản tin IPv6 đến đích, nếu Interface nào được chọn để gửi bản tin đi thì địa chỉ IPv6 của Interface đó được chọn làm địa chỉ nguồn cho bản tin.

Quy tắc 6 (Prefer matching label):

Địa chỉ nguồn nào có cùng giá trị Label với địa chỉ đích thì sẽ được chọn. Giá trị Label này được IETF quy định chi tiết trong một bảng riêng có tên gọi là Policy Table sẽ được trình bày sau.

Quy tắc 7 (Prefer temporary addresses):

Như đã trình bày, theo RFC 4941, các máy tính sẽ tạo thêm một địa chỉ Temporary Address có thời gian ngắn hơn dành cho kết nối từ máy tính ra bên ngoài nhằm nâng cao bảo mật. Vì thế địa chỉ Temporary Address sẽ được ưu tiên làm địa chỉ nguồn hơn so với địa chỉ Public Address.

Quy tắc 8 (Longest prefix matching):

Nếu địa chỉ nguồn nào có số bit (tính từ đầu) trùng với địa chỉ đích nhiều hơn thì sẽ được chọn. Như minh họa dưới đây thì địa chỉ A sẽ được chọn làm nguồn.

Nguồn A	**2001:db8:a029:1001:5221:473d:c012:1001**
Nguồn B	**2001:db8:a029:1001:5221:473d:c112:a001**
Đích D	**2001:db8:a029:1001:5221:473d:c012:a001**

Hình 53. Nguyên tắc Longest prefix matching giữa địa chỉ nguồn và đích

3.14. QUY TẮC 6: POLICY TABLE

Theo quy tắc số 6, địa chỉ nguồn IPv6 nào có cùng Label với địa chỉ đích thì sẽ được chọn, Label này được quy định trong bảng Policy Table. Bảng này bao gồm những Prefix phổ biến được quy định theo chức năng như địa chỉ IPv6 Loopback, Tunnel 6to4... Dưới đây là bảng Policy Table theo RFC 6724, một số Prefix không còn được dùng trong thực tế như Site-Local, 6Bone ...

```
C:\>netsh interface ipv6 show prefixpolicies
Querying active state...

Precedence   Label   Prefix
----------   -----   ------------------------------------------
        50       0   ::1/128          <---- Địa chỉ IPv6 Loopback
        40       1   ::/0             <---- Địa chỉ IPv6
        35       4   ::ffff:0:0/96    <---- Địa chỉ IPv4-mapped
        30       2   2002::/16        <---- Dành cho Tunnel 6to4
        20       5   2001::/32        <---- Dành cho Tunnel Teredo
        10       3   fc00::/7         <---- Địa chỉ ULA
         1      11   fec0::/10        <---- Địa chỉ IPv4-compatible
         1      12   3ffe::/16        <---- Địa chỉ Site-Local
         1       3   ::/96            <---- Địa chỉ mạng 6Bone
```

Hình 54. Chi tiết Policy Table

Các Prefix trong bảng này được xếp theo thứ tự ưu tiên, thông tin thể hiện mức ưu tiên là Precedence, giá trị Precedence càng lớn thì Prefix càng được ưu tiên. Vì địa chỉ IPv4 được cũng được so sánh với IPv6 để kiểm tra mức ưu tiên nên trong bảng này địa chỉ IPv4 được biểu diễn ở dạng IPv6-mapped ::ffff:0:0/96. Trong hình trên, địa chỉ IPv6 (::/0) có Precendence=40 nên được ưu tiên hơn địa chỉ IPv4 có Precedence=35.

Điều chú ý ở đây là các Prefix trong Policy Table được dùng để so sánh và xếp mức ưu tiên cho địa chỉ IPv6 đích. Việc so sánh tính theo số bit bên trái của địa chỉ đích trùng nhất (longest-matching) với Prefix nào có trong bảng Policy Table. Sau khi xác định được mức ưu tiên của địa chỉ đích thì xét tiếp giá trị bên cạnh là Label. Giá trị của Label không phải là thông tin để xét ưu tiên mà chỉ là một con số nhằm phân loại hay gán nhãn cho Prefix đó. Sau đó địa chỉ IPv6 nguồn cũng được so sánh để phân loại Label, địa chỉ nguồn nào có Label trùng với địa chỉ đích thì sẽ được chọn để khởi tạo kết nối.

Như vậy Precedence dùng để xếp loại ưu tiên của địa chỉ đích, sau đó sẽ dùng Label để chọn địa chỉ nguồn.

Chú ý:

- Những nội dung trình bày trên đây minh họa quy tắc lựa chọn địa chỉ nguồn IPv6 để thực hiện các kết nối đến một địa chỉ đích, điều này là do mỗi Interface nguồn có thể có nhiều loại địa chỉ IPv6 và thậm chí có cả IPv4.
- Các Interface đích cũng có nhiều địa chỉ tương tự. RFC 6724 cũng đưa ra các quy tắc lựa chọn địa chỉ đích cho việc thực hiện kết nối. Nội dung này không được trình bày chi tiết ở đây, bạn đọc có thể xem thêm thông tin ở RFC 6724.

3.15 TỔNG KẾT CHƯƠNG 3

Chương 3 đã trình bày một cách toàn diện và chi tiết về các loại địa chỉ IPv6, từ cấu trúc, cách biểu diễn đến các đặc điểm kỹ thuật nổi bật. IPv6 không chỉ mở rộng không gian địa chỉ lên 128 bit mà còn mang lại nhiều cải tiến vượt trội so với IPv4, bao gồm việc loại bỏ địa chỉ Broadcast, phân chia địa chỉ Multicast theo phạm vi (Scope) và đảm bảo địa chỉ Link-Local (LLA) không bị trùng lặp giữa các mạng dù chỉ sử dụng trong phạm vi nội bộ. Đặc biệt, địa chỉ Solicited-Node Multicast là một điểm nhấn quan trọng, tối ưu hóa hoạt động của giao thức IPv6 và nâng cao hiệu suất mạng.

Việc hiểu rõ các loại địa chỉ IPv6, bao gồm Unicast (GUA, ULA, LLA), Multicast, Anycast, cùng các quy tắc lựa chọn địa chỉ, không chỉ hỗ trợ quy hoạch và cấu hình mạng hợp lý mà còn tạo điều kiện để vận hành và khai thác hệ thống IPv6 hiệu quả trong thực tế. Những kiến thức này là nền tảng vững chắc để bạn đọc tiếp tục khám phá các giao thức và dịch vụ mạng IPv6 trong các chương tiếp theo.

3.16 CÂU HỎI ÔN TẬP CHƯƠNG 3

01

Tại sao IPv6 sử dụng hệ thập lục phân (Hexa) để biểu diễn địa chỉ và cách biểu diễn này có gì đặc biệt so với IPv4?

IPv6 sử dụng hệ thập lục phân vì địa chỉ IPv6 có độ dài 128 bit, lớn hơn nhiều so với địa chỉ IPv4 32 bit. Nếu biểu diễn bằng hệ thập phân, địa chỉ IPv6 sẽ quá dài và khó đọc (có thể lên đến 39 chữ số). Hệ thập lục phân cho phép biểu diễn 4 bit bằng một ký tự, giúp địa chỉ IPv6 được viết ngắn gọn hơn, chia thành 8 nhóm 16 bit (hextet) cách nhau bởi dấu hai chấm (:). Một điểm đặc biệt nữa là IPv6 cho phép rút gọn các số 0 đứng đầu mỗi hextet và thay thế một hoặc nhiều nhóm hextet toàn số 0 liên tiếp bằng dấu hai chấm kép (::), giúp địa chỉ trở nên dễ đọc và dễ nhớ hơn.

02

Địa chỉ IPv6 được phân loại như thế nào và sự khác biệt chính giữa các loại địa chỉ Unicast (GUA, ULA, LLA), Multicast và Anycast là gì?

Địa chỉ IPv6 được phân loại theo hai cách chính: theo cách thức hoạt động (Type) và phạm vi hoạt động (Scope). Sự khác biệt trong cách thức hoạt động của 3 loại trên là:

- **Unicast:** Đại diện cho một giao diện mạng duy nhất, truyền dữ liệu theo kiểu "một-đến-một". Có ba loại địa chỉ Unicast chính:
  - Global Unicast Address (GUA): Tương đương địa chỉ Public của IPv4, có phạm vi toàn cầu và thường được sử dụng trên Internet.
  - Unique Local Address (ULA): Tương đương địa chỉ Private của IPv4, chỉ có phạm vi nội bộ và không được định tuyến trên Internet.
  - Link Local Address (LLA): Là loại địa chỉ mới của IPv6, chỉ có phạm vi trong cùng một phân đoạn mạng (link) và không được router chuyển tiếp.
- **Multicast:** Đại diện cho một nhóm các giao diện mạng, truyền dữ liệu theo kiểu "một-đến-nhiều".
- **Anycast:** Đại diện cho một nhóm các giao diện mạng, nhưng chỉ một giao diện gần nguồn gửi nhất sẽ nhận được gói tin ("một-đến-một trong số nhiều"). Sự khác biệt chính nằm ở đối tượng nhận dữ liệu và phạm vi hoạt động của địa chỉ. Unicast gửi đến một địa chỉ duy nhất, Multicast gửi đến một nhóm, Anycast gửi đến một trong một nhóm và mỗi loại Unicast lại có phạm vi sử dụng khác nhau.

03

Địa chỉ Broadcast của IPv4 được thay thế bằng cơ chế nào trong IPv6?

IPv6 không còn sử dụng địa chỉ Broadcast theo cách truyền thống như IPv4. Thay vào đó, IPv6 sử dụng một địa chỉ Multicast đặc biệt là ff02::1 (All Nodes Link-Local) để gửi thông điệp đến tất cả các thiết bị trên cùng một phân đoạn mạng. Về bản chất, chức năng tương tự nhưng cách triển khai và quản lý hiệu quả hơn.

04

Địa chỉ Global Unicast (GUA) được cấu trúc như thế nào và những phần nào quan trọng trong việc quy hoạch mạng IPv6?

Địa chỉ GUA thường có cấu trúc gồm hai phần bằng nhau đều là 64 bit: Network Prefix và Interface ID. Phần Network Prefix lại được chia thành Global Routing Prefix và Subnet ID (cho phép tổ chức chia mạng con). Phần Interface ID (64 bit) thường được tạo tự động từ địa chỉ MAC (sử dụng EUI-64) hoặc ngẫu nhiên (trong SLAAC). Các phần quan trọng trong quy hoạch GUA bao gồm việc xác định kích thước Global Routing Prefix được cấp phát, thiết kế Subnet ID phù hợp với cấu trúc mạng nội bộ và đảm bảo tính duy nhất của Interface ID trên mỗi phân đoạn mạng.

05

Địa chỉ Unique Local Address (ULA) khác biệt như thế nào so với địa chỉ Private của IPv4 và tại sao nên sử dụng công cụ tạo địa chỉ ULA tự động?

Địa chỉ ULA tương ứng với địa chỉ Private của IPv4 về phạm vi hoạt động (chỉ trong mạng nội bộ), nhưng điểm khác biệt quan trọng là ULA được thiết kế để đảm bảo tính duy nhất trên toàn cầu, bảo đảm khi các mạng nội bộ kết nối với nhau. Điều này giúp tránh xung đột địa chỉ khi sáp nhập công ty hoặc kết nối VPN giữa các mạng sử dụng ULA. Việc sử dụng các công cụ tạo địa chỉ ULA tự động (ví dụ: "Unique Local IPv6 Generator") được khuyến khích để đảm bảo tính duy nhất của tiền tố FD00::/8 được tạo ngẫu nhiên, tránh việc quy hoạch trùng lặp thủ công.

06

Địa chỉ Link Local Address (LLA) có vai trò gì trong IPv6 và tại sao mỗi giao diện IPv6 đều cần có một địa chỉ LLA?

Địa chỉ LLA có vai trò quan trọng trong việc cho phép các thiết bị IPv6 trên cùng một phân đoạn mạng (link) có thể giao tiếp với nhau mà không cần cấu hình địa chỉ GUA hoặc ULA. Tất cả các giao diện IPv6 đều tự động có một địa chỉ LLA (thường bắt đầu bằng FE80::/10). LLA được sử dụng cho các giao thức như Neighbor Discovery Protocol (NDP) để tìm kiếm các thiết bị lân cận, phân giải địa chỉ MAC và phát hiện địa chỉ trùng lặp (DAD), cũng như để giao tiếp với DHCPv6 Server để lấy địa chỉ GUA hoặc ULA.

07

Quy tắc lựa chọn địa chỉ nguồn IPv6 (RFC 6724) hoạt động như thế nào khi một giao diện có nhiều địa chỉ IPv6 khác nhau?

Khi một thiết bị có nhiều địa chỉ IPv6 (ví dụ: GUA, ULA, LLA, Temporary Address) và cần khởi tạo một kết nối đến một địa chỉ đích, RFC 6724 định nghĩa một tập hợp các quy tắc để lựa chọn địa chỉ nguồn phù hợp nhất. Các quy tắc này được áp dụng theo thứ tự ưu tiên, bao gồm: ưu tiên địa chỉ trùng với địa chỉ đích, ưu tiên địa chỉ có phạm vi phù hợp nhất, tránh địa chỉ đã bị deprecated, ưu tiên địa chỉ Home Address (trong Mobile IPv6), ưu tiên địa chỉ của giao diện gửi đi, ưu tiên địa chỉ có cùng label (theo Policy Table), ưu tiên địa chỉ tạm thời (Temporary Address) và cuối cùng là ưu tiên địa chỉ có tiền tố trùng khớp dài nhất với địa chỉ đích.

08

Địa chỉ Solicited-Node Multicast được tạo ra như thế nào và tại sao nó là một cải tiến quan trọng trong IPv6?

Địa chỉ Solicited-Node Multicast được tạo ra tự động từ địa chỉ Unicast của một giao diện. Nó được hình thành bằng cách lấy 24 bit cuối cùng của địa chỉ Unicast và kết hợp với tiền tố ff02:0:0:0:0:1:ff00::/104. Mỗi địa chỉ Unicast trên một giao diện sẽ có một địa chỉ Solicited-Node Multicast tương ứng. Đây là một cải tiến quan trọng vì nó được sử dụng trong giao thức Neighbor Solicitation (một phần của NDP) để gửi truy vấn chỉ đến một nhóm nhỏ các node có khả năng có địa chỉ IP mục tiêu (dựa trên 24 bit cuối), thay vì gửi Broadcast đến tất cả các node trên mạng như trong ARP của IPv4. Điều này giúp giảm thiểu lưu lượng mạng và tăng hiệu suất.

PHẦN 1 – LÝ THUYẾT

CHƯƠNG 4

GIAO THỨC ICMPv6, NDP VÀ CÁC KỸ THUẬT, DỊCH VỤ MẠNG PHỔ BIẾN

CHƯƠNG 4

GIAO THỨC ICMPv6, NDP & CÁC KỸ THUẬT, DỊCH VỤ MẠNG PHỔ BIẾN

Giao thức IP đóng vai trò rất quan trọng trong việc định nghĩa địa chỉ mạng và thực hiện chuyển tiếp gói tin giữa các thiết bị định tuyến từ nguồn đến đích. Tuy nhiên, bản thân giao thức IP không có các cơ chế để giám sát, chẩn đoán và xử lý sự cố phát sinh trong quá trình truyền dữ liệu. Ví dụ, khi dữ liệu đã được truyền đi, giao thức IP không biết dữ liệu có đi đến đích được không, nếu không đến thì lý do là gì hay làm sao để biết một thiết bị đang hoạt động hay không hoặc cần kiểm tra chất lượng đường truyền có tốt không? Để khắc phục những hạn chế này, giao thức ICMP (Internet Control Message Protocol) ra đời nhằm hỗ trợ IP trong việc báo lỗi, kiểm tra kết nối và giám sát chất lượng đường truyền.

Khi IPv6 ra đời giao thức ICMP không những bị loại bỏ mà còn được phát triển, bổ sung và đóng vai trò quan trọng hơn. ICMPv6 trở thành một thành phần cốt lõi trong hầu hết các dịch vụ mạng IPv6, giúp loại bỏ các cơ chế không hiệu quả của IPv4 và bổ sung những tính năng mới mạnh mẽ hơn. Các giao thức quan trọng khác như Neighbor Discovery Protocol (NDP) và Multicast Listener Discovery (MLD) cũng được xây dựng dựa trên nền tảng của ICMPv6.

Nội dung chương 4 tập trung vào giao thức ICMPv6, Neighbor Discovery Protocol (NDP) và các kỹ thuật, dịch vụ mạng phổ biến liên quan đến IPv6. Chương này bắt đầu bằng cách giải thích vai trò của ICMPv4 và tầm quan trọng của ICMPv6 như một thành phần cốt lõi của mạng IPv6. Tiếp theo, tài liệu đi sâu vào giao thức NDP, thay thế ARP của IPv4 và các cơ chế tự động cấu hình địa chỉ như SLAAC và DHCPv6. Cuối cùng, chương này trình bày các kỹ thuật quan trọng như PMTU Discovery và Duplicate Address Detection, cung cấp kiến thức nền tảng để quản lý và tối ưu hóa mạng IPv6.

QUA CHƯƠNG NÀY BẠN SẼ NẮM ĐƯỢC NHỮNG KIẾN THỨC SAU:

Hiểu lý do ICMPv6 trở thành một **thành phần cốt lõi** trong hầu hết các dịch vụ mạng IPv6, giúp loại bỏ các cơ chế không hiệu quả của IPv4.

Hiểu về giao thức mới Neighbor Discovery Protocol **(NDP)** và Multicast Listener Discovery **(MLD)** được xây dựng dựa trên nền tảng của ICMPv6 ra sao.

Hiểu **cấu trúc và các nhóm bản tin** ICMP Query Message và Error Message phổ biến.

Kỹ thuật **gán địa chỉ tự động SLAAC** (Stateless Address Autoconfiguration), cho phép thiết bị tự động tạo địa chỉ IPv6 mà không cần DHCP.

Sự kết hợp giữa **SLAAC và DHCPv6** và mô hình Stateful DHCPv6. Bạn cũng sẽ hiểu về các phương thức định danh DHCPv6 Client như DUID và IAID.

Kỹ thuật EUI-64 để tạo Interface-ID từ địa chỉ MAC48 và **RFC 4941** với phương pháp tạo Interface-ID ngẫu nhiên, địa chỉ chính và địa chỉ tạm thời.

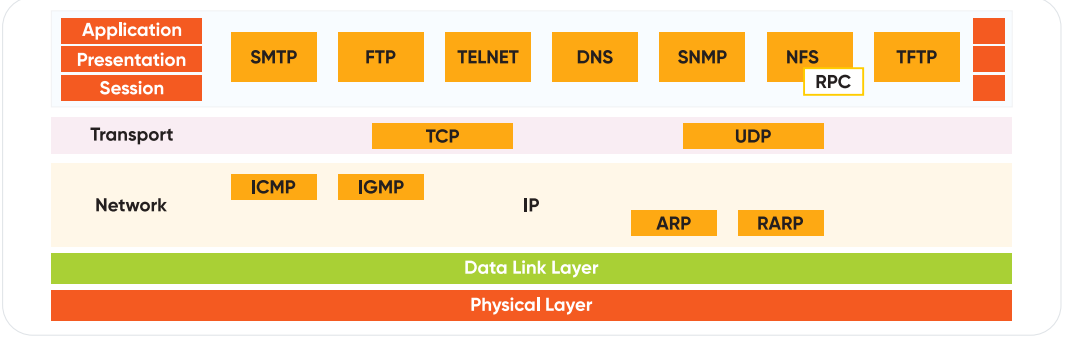
Các **trạng thái hoạt động** của địa chỉ IPv6: Tentative, Valid, Preferred, Deprecated và Invalid.

Kỹ thuật **phân giải địa chỉ MAC** sử dụng giao thức NDP (thay thế ARP), **kiểm trùng địa chỉ** DAD (Duplicate Address Detection) và **dò tìm IPv6 Path MTU (PMTU)**.

4.1. TỔNG QUAN VỀ GIAO THỨC ICMP

Giao thức ICMP (Internet Control Message Protocol), được mô tả chi tiết trong tài liệu RFC 792, là một thành phần quan trọng của bộ giao thức TCP/IP. Giao thức này hoạt động như một công cụ hỗ trợ cho IPv4 nên được gọi là ICMPv4. Với vai trò chính là truyền tải các thông điệp báo lỗi và chẩn đoán, ICMP giúp các thiết bị mạng phát hiện và khắc phục sự cố kết nối, đảm bảo luồng thông tin được thông suốt và tin cậy.

ICMP được tích hợp trong IPv4 nên mọi thiết bị sử dụng IPv4 đều có sẵn ICMP mà không cần phải cài đặt hay khai báo gì thêm. Nhờ đó, ICMP trở thành một công cụ thiết yếu trong việc giám sát và duy trì hoạt động mạng, hỗ trợ các chức năng quan trọng như kiểm tra độ trễ, xác minh kết nối, báo cáo lỗi định tuyến và cung cấp thông tin về trạng thái hoạt động của mạng.

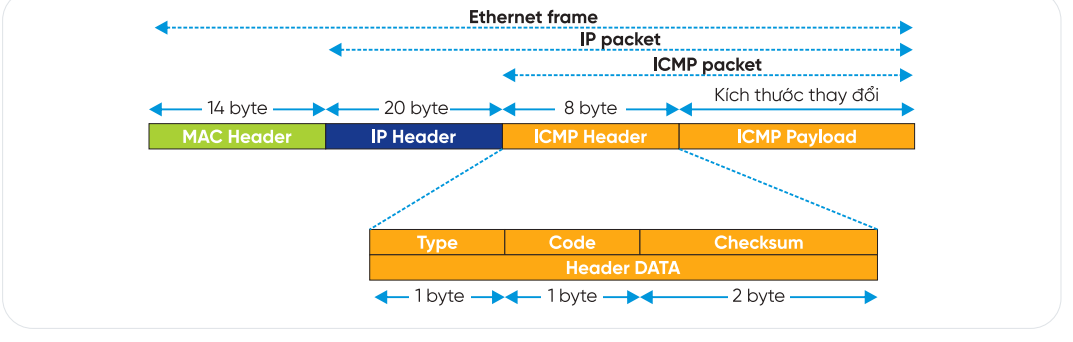


Hình 55. Giao thức IP và các giao thức hỗ trợ

ICMP (Internet Control Message Protocol) hoạt động ở lớp 3 trong mô hình OSI, cùng với giao thức IP và được truyền tải trực tiếp qua IP. Không giống như IP – được thiết kế để truyền dữ liệu giữa các thiết bị mạng – ICMP chủ yếu đảm nhận vai trò gửi các thông báo và chẩn đoán lỗi giữa các node mạng. Các thông điệp của ICMP được sử dụng để báo hiệu khi có sự cố xảy ra, giúp xác định các vấn đề về kết nối hoặc hiệu suất mạng.

Tuy nhiên, ICMP chỉ gửi thông báo về những gói tin IP gặp lỗi, chẳng hạn như khi một gói tin không thể tới đích do lỗi định tuyến hoặc các vấn đề liên quan đến TTL (Time to Live). Đặc biệt, nếu một gói tin ICMP gặp lỗi trong quá trình truyền tải, sẽ không có bất kỳ thông báo nào gửi lại để báo hiệu lỗi của chính nó. Điều này giúp ngăn việc lặp lại các thông báo lỗi không cần thiết và giảm tải cho mạng, đảm bảo hiệu quả và tối ưu hóa luồng thông tin giữa các thiết bị.

Cấu trúc của bản tin ICMP gồm ICMP Header và Payload, bản tin này sẽ được đóng gói bởi IP Header và Ethernet Header để truyền tải trong mạng. Các thành phần và kích thước của bản tin ICMP được minh họa trong hình sau.



Hình 56. Cấu trúc bản tin ICMP

Trong ICMP Header, hai trường quan trọng là Type và Code. Type dùng để phân nhóm bản tin ICMP, tương ứng với mỗi nhóm sẽ có nhiều bản tin phục vụ các mục đích khác nhau và được đặt mã Code riêng. Phần dữ liệu cho ICMP Header cũng thay đổi tùy theo loại bản tin, còn phần Checksum giúp kiểm tra lỗi bản tin ICMP.

4.2. PHÂN LOẠI BẢN TIN ICMP

Có rất nhiều loại bản tin ICMP được đề xuất nhưng chỉ một số loại được dùng phổ biến trong thực tế còn phần lớn không còn được sử dụng nữa (Deprecated). Tương tự số bản tin trong mỗi loại cũng khá nhiều và chỉ một số là được sử dụng trong thực tế. Dưới đây là danh sách những nhóm bản tin ICMP được sử dụng phổ biến nhất cùng với chi tiết bản tin của từng nhóm với giá trị Code quy định.

Type	Code	Description
0 – Echo Reply	0	Echo reply (used to ping)
3 – Destination Unreachable	0	Destination network unreachable
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
	4	Fragmentation required, and DF flag set
	5	Source route failed
	6	Destination network unknown
	7	Destination host unknown
	8	Source host isolated
	9	Network administratively prohibited
	10	Host administratively prohibited
	11	Network unreachable for ToS
	12	Host unreachable for ToS
	13	Communication administratively prohibited
	14	Host Precedence Violation
	15	Precedence cutoff in effect

Type	Code	Description
4 – Source Quench	0	Source quench (congestion control)
5 – Redirect Message	0	Redirect Datagram for the Network
	1	Redirect Datagram for the Host
	2	Redirect Datagram for the ToS & network
	3	Redirect Datagram for the ToS & host
8 – Echo Request	0	Echo request (used to ping)
9 – Router Advertisement	0	Router Advertisement
10 – Router Solicitation	0	Router discovery/selection/solicitation
11 – Time Exceeded	0	TTL expired in transit
	1	Fragment reassembly time exceeded
12 – Parameter Problem: Bad IP header	0	Pointer indicates the error
	1	Missing a required option
	2	Bad length
13 – Timestamp	0	Timestamp
14 – Timestamp Reply	0	Timestamp reply
17 – Address Mask Request	0	Address Mask Request
18 – Address Mask Reply	0	Address Mask Reply

Bảng 6. Chi tiết các bản tin ICMP

Dù có nhiều nhóm bản tin như vậy nhưng xét về chức năng thì các nhóm bản tin ICMP được phân thành hai nhánh chính (Category) là:

Querry Message:

Một thiết bị gửi bản tin truy vấn (Querry) đến một thiết bị khác và yêu cầu phản hồi (Reply) thông tin. Những bản tin thuộc nhánh này thường dùng để kiểm tra và chẩn đoán các sự cố mạng.

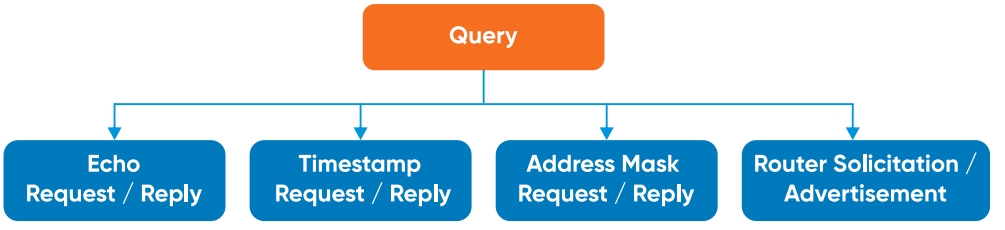
Error Report Message:

Khi một thiết bị phát hiện lỗi trong quá trình truyền các gói tin IP, thiết bị đó sẽ tự tạo một bản tin mô tả nguyên nhân lỗi và thông báo cho thiết bị nguồn (Sender/Source) của những gói tin IP lỗi này mà không cần bản tin yêu cầu nào.

4.3. CÁC NHÓM BẢN TIN ICMP QUERRY MESSAGE

Các bản tin loại này được dùng để trao đổi thông tin giữa các node mạng nhằm phục vụ một tính năng nào đó của giao thức IP (như MTU, Neighbor Discovery, Router Advertisement ..) hoặc để phục vụ việc kiểm tra/chẩn đoán lỗi mạng (như Ping, Tracert ...).

Không như ICMP Error Massage được tự động gửi đi khi có sự cố, các bản tin thuộc loại Query Message chỉ được tạo ra bởi một ứng dụng (ví dụ giám sát mạng) hoặc theo định kỳ nhằm cung cấp thông tin cho các thiết bị khác (ví dụ Router Advertisement) hoặc nhằm phản hồi theo yêu cầu (ví dụ Echo/Reply).



Hình 57. Chi tiết nhóm bản tin ICMP Querry

Chi tiết 4 nhóm bản tin thuộc Query Message như sau:

Echo Request (Type 8) và Echo Reply (Type 0)

Đây là 2 bản tin được nhiều người biết đến nhất trong tất cả bản tin ICMP và cả 2 được tích hợp thành công cụ chẩn đoán mạng phổ biến nhất là lệnh PING. Khi máy A thực hiện lệnh PING đến địa chỉ máy B thì một gói tin ICMP Echo Request được gửi đến máy B. Máy B sau khi nhận được Request sẽ phản hồi bằng gói tin ICMP Echo Reply cho máy A. Trường hợp máy A không nhận được phản hồi từ máy B thì có khả năng máy B đang bị sự cố hay có thiết bị chặn ICMP hoặc lỗi tại một thiết bị trung gian nào đó (sau đó có thể dùng lệnh Tracert để kiểm tra tiếp).

Timestamp Request (Type 13) và Reply (Type 14)

Hai bản tin này được dùng để đồng bộ thời gian giữa 2 node mạng, trong đó một node sẽ gửi bản tin Timestamp Request và node kia sẽ phản hồi bằng Timestamp Reply. Hiện các bản tin này không còn được sử dụng và được thay thế bởi giao thức NTP (Network Time Protocol) hoặc PTP (Precision Time Protocol).

Mask Request (Type 17) và Mask Reply (Type 18)

Hai bản tin này trước đây được triển khai cho các máy trạm không đĩa cứng (Diskless) nhằm xác định Subnet mask mà hệ thống mạng hiện tại đang dùng. Một máy trạm khi khởi động sẽ gửi bản tin Mask Request, sau đó một router sẽ phản hồi địa chỉ Subnet mask bằng gói tin Mask Reply. Mạng Diskless hầu như không còn dùng trong thực tế nên các bản tin này cũng vậy.

Router Solicitation (Type 10) và Router Advertisement (Type 9)

Nếu một máy tính không được khai báo cố định Default Gateway (sẽ bị mất sau khi khởi động lại) hoặc router làm Default Gateway bị sự cố thì cần phải có cơ chế tự động tìm kiếm một router mới làm Default Gateway. Bản tin ICMP Router Solicitation sẽ được sử dụng trong trường hợp này, địa chỉ đích là địa chỉ Multicast 224.0.0.2, đại diện cho tất cả các router trên cùng phân đoạn mạng, được máy tính gửi đi để truy vấn (Query) xem có router nào đang hoạt động không.

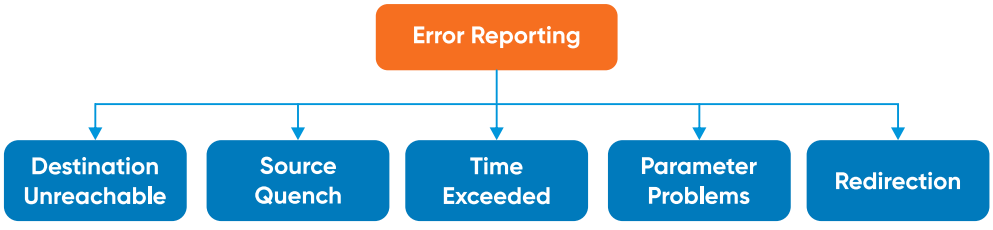
Các router khi nhận được bản tin trên, sẽ tự động phản hồi lại địa chỉ của mình bằng gói tin router Advertisement (Type=9) về lại cho máy tính. Định kỳ các router cũng tự động gửi bản tin router Advertisement để tự quảng bá chính mình cho các Host.

Đối với IPv4 thì hai bản tin này không được sử dụng nhiều nhưng với IPv6, chúng đóng vai trò rất quan trọng như: cho phép tự cấu hình địa chỉ IP (dịch vụ SLAAC), thay thế ARP bằng giao thức NDP, giúp kiểm trùng địa chỉ (Duplicated) ...

4.4. CÁC NHÓM BẢN TIN ICMP ERROR MESSAGE

Các bản tin ICMP Error Message được tạo ra khi việc truyền các gói tin IP có vấn đề. Node mạng tạo ra bản tin này là node mạng đích hoặc có thể là node mạng trung gian. Có một số quy tắc để tạo ra bản tin loại này như sau:

- Không gửi thông báo lỗi cho gói tin IP chứa bản tin ICMP (thường có IP Protocol = 1) mà chỉ thông báo lỗi cho những gói tin IP chứa dữ liệu.
- Không gửi thông báo lỗi cho gói tin IP có địa chỉ đích là Broadcast hoặc Multicast address.
- Không gửi thông báo lỗi cho gói tin IP có địa chỉ nguồn không xác định ví dụ: 127.0.0.1 hoặc 0.0.0.0.
- Nếu gói tin bị phân mảnh (Fragemented) và có lỗi thì chỉ thông báo lỗi cho gói tin bị phân mảnh đầu tiên (thường có Fragement Offset = 0).



Hình 58. Chi tiết nhóm bản tin ICMP Querry

Có 5 loại bản tin thuộc ICMP Error Message, mỗi loại có chức năng sau:

Destination unreachable (Type 3)

Khi một node mạng phát hiện không thể tìm thấy (Unreachable), các thông tin liên quan đến node mạng đích như: địa chỉ IP, loại Protocol hay Port đích của gói tin IPv4 thì nó sẽ gửi bản tin ICMP Type = 3 về lại cho node mạng nguồn.

Nguyên nhân Unreachable có thể do node mạng đích bị sự cố không còn hoạt động, không tìm thấy Route trỏ đến địa chỉ IP đích hoặc TCP/UDP Port đích trong gói tin IP không được tìm thấy tại node mạng đích. Chi tiết từng nguyên nhân gây ra lỗi Unreachable sẽ được chỉ rõ bằng Code và bản tin này có nhiều Code nhất so với các loại bản tin khác.

Source quench (Type 4)

Một node mạng khi nhận thấy bộ đệm dành cho việc nhận gói tin (Buffer) sắp tới ngưỡng tràn hoặc bị tràn thì nó sẽ gửi gói tin ICMP Source Quench cho node nguồn để yêu cầu giảm tốc độ truyền. Khi node nguồn nhận Source Quench nó tự động giảm tốc độ truyền cho đến khi hết nhận Source Quench. Sau đó một thời gian node nguồn sẽ tăng lại dần cho đến tốc độ ban đầu.

Việc kiểm soát tốc độ truyền bằng ICMP Source quench được chứng minh là không hiệu quả nên đã không được sử dụng trong thực tế, nội dung này được mô tả trong RFC 6633.

Time Exceeded (Type 11)

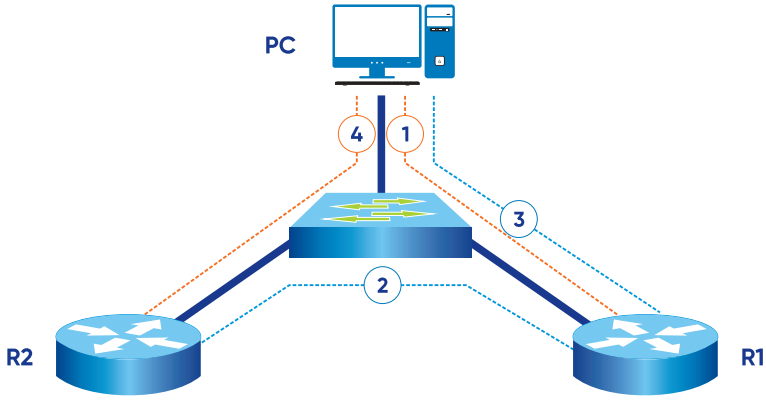
Để phòng chống tình trạng gây lặp vòng (Loop) các bản tin trong mạng gây ra quá tải cho các thiết bị thì giao thức IP đã đưa ra cơ chế để hạn chế gói tin bị lặp vòng là sử dụng thuộc tính Time-to-Live (TTL) của IPv4 (và Hop-limit của IPv6). Khi một router nhận được gói tin IP nó sẽ giảm giá trị TTL của gói tin đó đi 1 giá trị trước khi chuyển đi tiếp. Nếu một router nào đó nhận gói tin có TTL=0 thì nó sẽ loại bỏ gói tin và gửi bản tin ICMP Time Exceeded về cho node nguồn.

Parameter Problem (Type 12):

Phần Header của mỗi gói tin IP có trường Header Checksum để các thiết bị kiểm tra lỗi trong quá trình truyền. Nếu một node mạng kiểm tra trường này và phát hiện lỗi thì nó sẽ loại bỏ bản tin IP và gửi gói tin ICMP Parameter Problem để thông báo về cho node nguồn.

Redirection (Type 5):

Hình dưới sẽ minh họa cho hoạt động của bản tin này. Khi một PC truyền dữ liệu đến Default Gateway R1 (bước 1), nếu R1 phát hiện R2 có hướng đi đến đích tốt hơn thì nó sẽ thực hiện chuyển tiếp các gói tin đến R2 (bước 2), đồng thời gửi Next-hop mới về cho PC (bước 3) thông qua gói tin ICMP Redirection. PC sẽ cập nhật Next-hop mới và gửi các gói tin tiếp theo trực tiếp đến R2 (bước 4).



Hình 59. Hoạt động của bản tin ICMP Redirect

Gói tin ICMP Redirection chỉ được gửi từ router đến Host, không được gửi giữa router và router. Trong thực tế bản tin này không được sử dụng vì ảnh hưởng đến bảo mật. Đối với Cisco router dùng lệnh "no ip redirect" để ngăn gửi bản tin ICMP này.

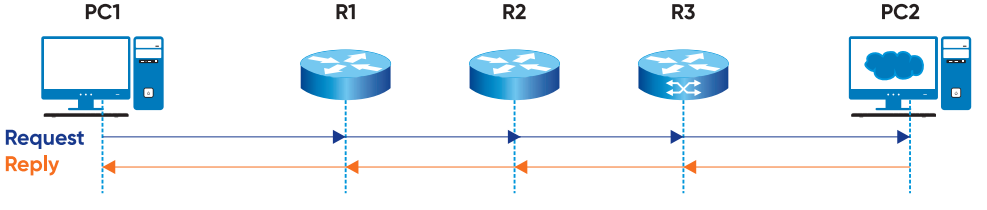
4.5. MỘT SỐ CÔNG CỤ, KỸ THUẬT SỬ DỤNG ICMP

Trên cơ sở nguyên tắc hoạt động của các bản tin ICMP, một số công cụ chẩn đoán mạng đã được tạo ra. Sau đây là một số công cụ được sử dụng khá phổ biến trong thực tế:

4.5.1. Lệnh PING

Đây là lệnh cơ bản nhất để kiểm tra kết nối giữa 2 node mạng có tồn tại hay không và đồng thời cũng kiểm tra độ trễ (RTT – Round Time Trip) là thời gian gói tin đi về giữa hai node mạng.

Lệnh PING sử dụng kết hợp cả hai bản tin Echo Request (Type=8) do node nguồn gửi đi và Echo Reply (Type=0) do node đích phản hồi. Nếu bản tin Echo Reply không được trả về có nghĩa: Node mạng đích bị không hoạt động hoặc bản tin ICMP bị chặn tại Firewal trung gian.



Hình 60. Các bản tin trong lệnh Ping

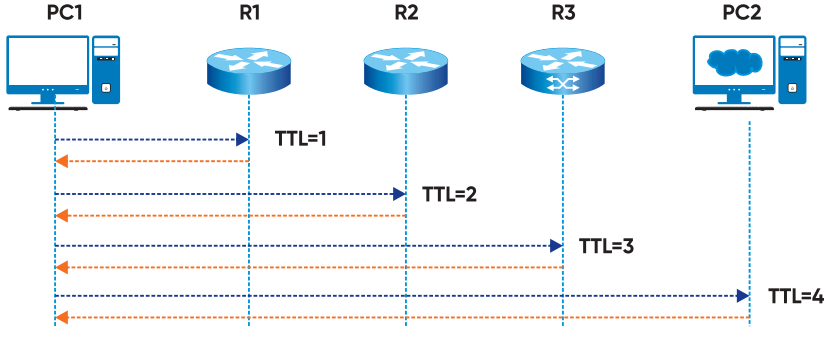
```
C:\>ping google.com

Pinging google.com [2404:6800:4005:822::200e] with 32 bytes of data:
Reply from 2404:6800:4005:822::200e: time=24ms
Reply from 2404:6800:4005:822::200e: time=25ms
Reply from 2404:6800:4005:822::200e: time=23ms
Reply from 2404:6800:4005:822::200e: time=25ms

Ping statistics for 2404:6800:4005:822::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 25ms, Average = 24ms
```

Hình 61. Thông tin trả về của lệnh Ping

4.5.2. Lệnh TRACERT/TRACEROUTE:

Lệnh Tracert/Traceroute là công cụ được dùng phổ biến để để chẩn đoán lỗi kết nối mạng bằng cách xác định đường đi của gói tin từ node nguồn đến đích sẽ đi qua những node mạng trung gian nào.

Cách hoạt động của lệnh này cũng sử dụng 2 bản tin Echo Request và Echo Reply như lệnh Ping nhưng kết hợp thông minh với thuộc tính TTL (Time-to-Live) của gói tin IP và bản tin ICMP Time-Exceeded (TE).



Hình 62. Chi tiết hoạt động của lệnh Trace

Node nguồn sẽ lần lượt gửi bản tin ICMP Echo Request có địa chỉ đích là của node đích (PC2) với TTL lần lượt là 1, 2, 3, 4 .... cho đến khi nhận được gói tin Echo Reply. Với TTL=1, 2, 3 ... thì tại các router trung gian 1, 2, 3 ... các gói tin có giá trị TTL=0 vì thế router trung gian này sẽ tự khởi tạo gói tin ICMP Time-Exceeded thông báo về lại cho node nguồn, nhờ đó node nguồn có thể biết gói tin đi lần lượt qua những router nào. Mỗi lần gửi bản tin Echo Request đi và nhận bản tin Time Exceeded về thì node nguồn có thể tính được cả độ trễ RTT.

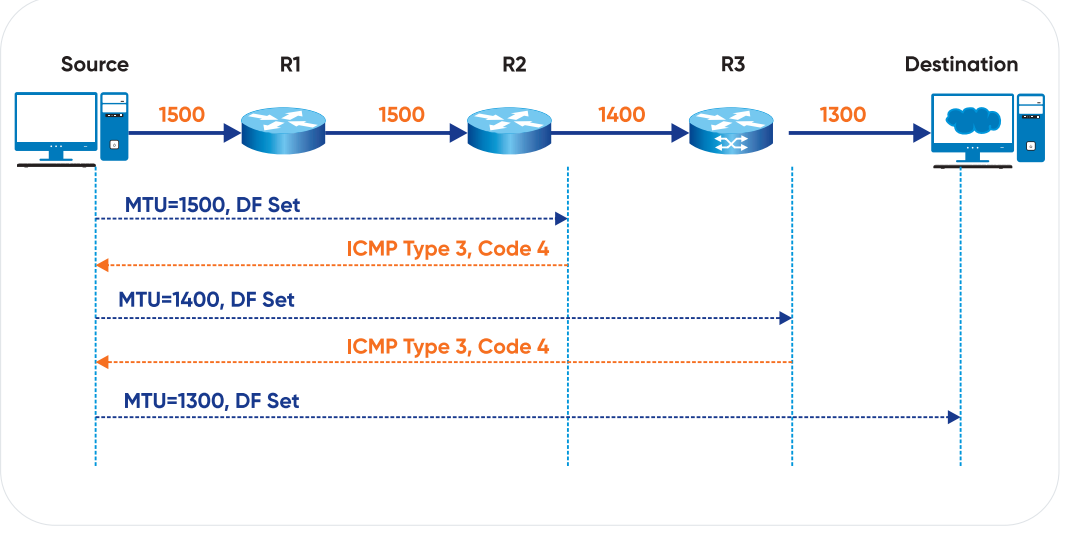
```
C:\>tracert www.google.com

Tracing route to www.google.com [2404:6800:4005:804::2004]
over a maximum of 30 hops:

1    2 ms     2 ms     2 ms     2001:dc8:9000:14::1
2    4 ms     3 ms     4 ms     2001:dc8:9000:1::17
3    29 ms    4 ms     4 ms     2001:dc8:9000::1
4    *        *        *        Request timed out.
5    5 ms     4 ms     4 ms     2001:de8:c::4:5899:1
6    21 ms    23 ms    23 ms    peer-as45899.pr02.hkg1.tfbnw.net [2620:0:1cff:dead:beee::1ed]
7    *        *        *        Request timed out.
8    24 ms    21 ms    22 ms    2404:6800:8264:1c0::1
9    24 ms    22 ms    22 ms    hkg07s33-in-x04.1e100.net [2404:6800:4005:804::2004]

Trace complete.
```

Hình 63. Thông tin trả về của lệnh Trace

4.5.3. Kỹ thuật Path MTU Discovery (PMTUD)

MTU (MTU - Maximum Transmission Unit) là kích thước lớn nhất mà một gói tin IP được phép truyền đi trên một Interface. Giá trị MTU phụ thuộc vào giao thức truyền dữ liệu lớp 2 như Ethernet, ATM ... hoặc giao thức đóng gói lớp 3 khác như GRE Tunnel hay IPSec VPN. Như vậy các kết nối từ điểm nguồn đến đích có thể có giá trị MTU khác nhau, nếu gói tin IP gửi đi có giá trị MTU lớn hơn của kết nối nào đó thì bản tin IP sẽ bị phân mảnh hoặc loại bỏ. Điều này sẽ ảnh hưởng đến việc truyền dữ liệu. PMTUD là kỹ thuật xác định kích thước MTU để một gói tin có thể truyền từ nguồn tới đích mà không bị phân mảnh hoặc loại bỏ, điều này giúp tăng tốc độ truyền, giảm độ trễ và tối ưu hiệu suất hoạt động của các node mạng.

Kỹ thuật PMTU được mô tả trong RFC 1191 cho IPv4 và RFC 8201 cho IPv6. Nguyên tắc hoạt động của kỹ thuật này kết hợp hai tính năng: Bật (Set=1) bit DF (Don't Fragment) trong phần Header của gói tin IP và sử dụng bản tin thông báo lỗi ICMP Type 3, Code 4 (Destination Unreachable + Fragmentation needed but DF set) để yêu cầu chỉnh lại MTU cho bản tin IP.



Hình 64. Chi tiết hoạt động của PMTU

Node nguồn sẽ thực hiện điều chỉnh kích thước gói tin IP theo MTU mới với DF=1 và gửi lại. Nếu không nhận được bản tin ICMP Type 3, Code 4 nào nữa thì node nguồn có thể xác định được giá trị MTU nhỏ nhất cần truyền đến đích một cách hiệu quả.

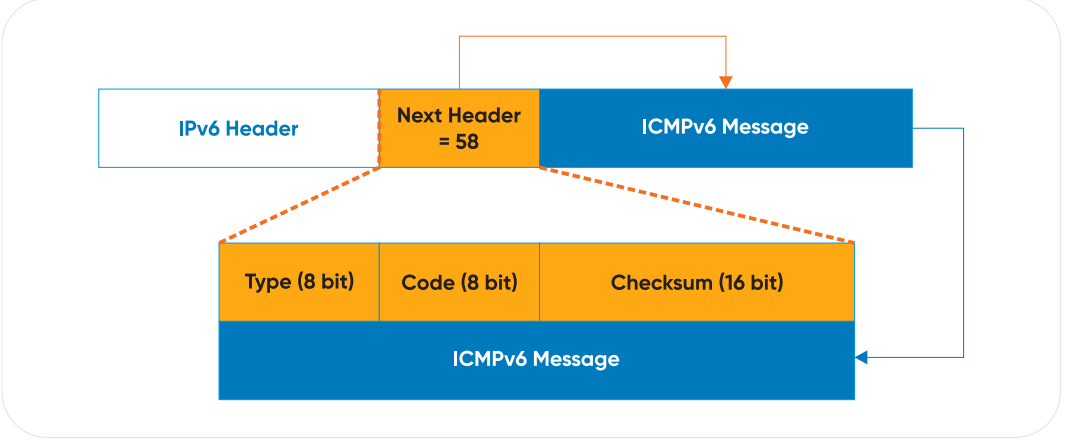
Chú ý:

- Một số công cụ khác (có sẵn trong hệ điều hành hay cài thêm) cũng hoạt động dựa trên cơ sở của ICMP như PathPing, TracePath, TraceTCP ...
- Nếu một node mạng (ví dụ Firewall, Router) chặn gói tin tất cả các bản tin ICMP thì kỹ thuật PMTUD không thể hoạt động được và có thể tạo ra ICMP Black-hole. Đây là tình trạng một node mạng liên tục nhận các gói tin có MTU vượt quá mức cho phép và có DF=1 khiến cho node mạng đó bị quá tải dẫn đến sinh ra sự cố mạng.

4.6. GIAO THỨC ICMPV6

Đây không chỉ là giao thức hỗ trợ cho IPv6 mà vai trò và tính năng của giao thức này cũng rất quan trọng. Chính ICMPv6 đã giúp loại bỏ một số giao thức cũ hoạt động không hiệu quả trên IPv4 như ARP, IGMP và thay vào đó các giao thức mới. Có thể nói, nếu không nắm được đặc điểm của ICMPv6 thì chúng ta không thể hiểu được hoạt động của một số giao thức hay kỹ thuật trên nền IPv6.

Giao thức ICMPv6 được mô tả trong RFC 4443 (thay thế cho RFC 2463 và RFC 1885 trước đó). Phần Header của bản tin ICMPv6 có Next Header=58.



Hình 65. Định dạng chung của bản tin ICMPv6

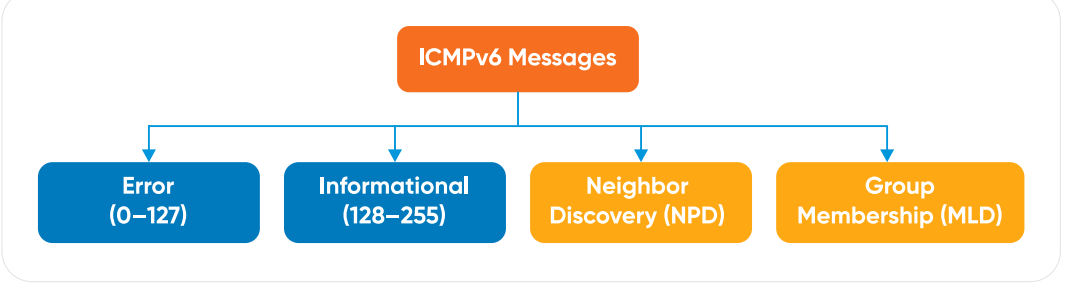
Cũng như ICMP, giao thức ICMPv6 vẫn được chia thành hai phân nhóm chính:

Error Message:

Mục đích của phân nhóm này nhằm thông báo lỗi giống như của ICMP Error Message. Các bản tin ICMPv6 loại này có giá trị Type được quy định từ 0 đến 127.

Informational Message:

Phân nhóm này cũng tương tự ICMP Query Message và có giá trị Type từ 128 đến 255.



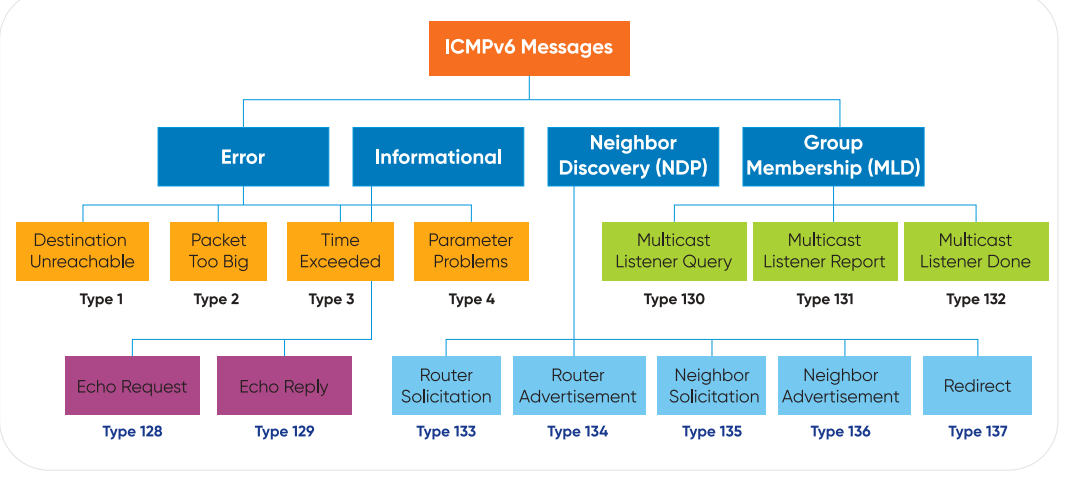
Hình 66. Hai nhóm bản tin chính của ICMPv6 và của NDP, MLD

Nhiều bản tin ICMP ít được sử dụng hoặc không hiệu quả đã bị loại bỏ khi chuyển sang ICMPv6 nên số lượng bản tin ICMPv6 sẽ ít hơn. Dưới đây là bảng so sánh những bản tin của ICMP và ICMPv6.

Group	Message	ICMPv4	ICMPv6
Error Message	Destination Unreachable	Có	Có
	Source Quench	Có	Không
	Packet Too Big	Không	Có
	Time Exceeded	Có	Có
	Parameter Problem	Có	Có
Informational Message	Echo Request	Có	Có
	Echo Reply	Có	Có
	Timestamp Request	Có	Không
	Timestamp Reply	Có	Không
	Mask Request	Có	Không
	Mask Reply	Có	Không

Bảng 7. So sánh các bản tin giữa ICMPv4 và ICMPv6

Một số giao thức không hiệu quả khác của IPv4 cũng bị thay thế khi chuyển sang IPv6. Giao thức ARP bị thay thế bởi NDP (Neighbor Discovery Protocol, RFC 4861) và giao thức IGMP bị thay bởi MLD (Multicast Listener Discovery, RFC 2710). Như vậy ngoài RFC 4443 mô tả cấu trúc một số bản tin của giao thức ICMPv6 thì các RFC 2710 và RFC 4861 cũng giới thiệu thêm một số bản tin ICMPv6 mới để phục vụ cho hoạt động của mình. Dưới đây là mô hình phân nhóm các loại bản tin ICMPv6 được mô tả trong các RFC 4443, RFC 2710 và RFC 4861.

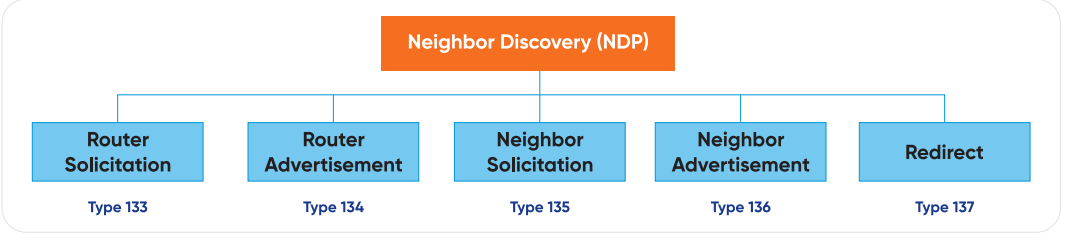


Hình 67. Chi tiết các bản tin của ICMPv6 và NDP, MLD

Giao thức MLD liên quan đến việc quản lý và truyền tải dữ liệu Multicast (như Tivi và Video trực tuyến) trong hệ thống mạng và chỉ được dùng trong một số hệ thống lớn như của nhà mạng nên sẽ không đề cập trong cuốn sách này. Giao thức NDP thay thế cho ARP là hoạt động không thể thiếu trong mạng IPv6 nên sẽ được trình bày chi tiết ở phần sau.

4.7. GIAO THỨC NDP

NDP là giao thức thay thế cho ARP có nhiệm vụ phân giải địa chỉ IPv6 sang địa chỉ MAC. NDP không sử dụng cấu trúc bản tin riêng như ARP mà dùng chính bản tin ICMPv6 với cấu trúc linh hoạt để làm nền tảng hoạt động cho mình.



Hình 68. Chi tiết của các bản tin của NDP

NDP sử dụng năm bản tin ICMPv6 trong đó có bốn bản tin làm việc theo cặp. Bốn bản tin này được sử dụng phổ biến trong một số dịch vụ mạng quan trọng của IPv6 và giúp các dịch vụ hoạt động này đơn giản và hiệu quả. Về cấu trúc, NDP hoàn toàn sử dụng cấu trúc của bản tin ICMPv6 nhưng chỉ có các Type khác nhau.

Router Advertisement

ETH	SRC MAC: **000D.DDDD.DDDD**	
	DEST MAC: **000D.DDDD.DDDD**	
IPv6	SRC IP: **FE80::20D:DDFF:FEDD:DDDD**	
	DEST IP: **FF02::1**	
ICMPv6	TYPE: **134**	CODE: **0**
	PREFIX: **2001:1234:A:B::/64**	
	MTU: **1500**	
	LINK LAYER ADDRESS: **000D.DDDD.DDDD**	

Neighbor Advertisement

ETH	SRC MAC: **000C.CCCC.CCCC**	
	DEST MAC: **000A.0AAA.0AAA**	
IPv6	SRC IP: **FE80::20C:CCFF:FECC:CCCC**	
	DEST IP: **FE80::20A:AFF:FEAA:AAA**	
ICMPv6	TYPE: **136**	CODE: **0**
	TARGET: **FE80::20C:CCFF:FECC:CCCC**	
	LINK LAYER ADDRESS: **000C.CCCC.CCCC**	

Hình 69. Cấu trúc 2 bản tin Router Solicitation và Router Advertisement

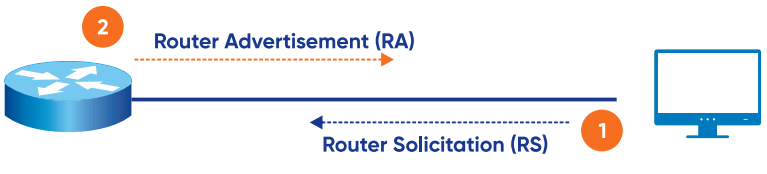
Chi tiết các bản tin của NDP như sau:

Router Solicitation (RS):

Bản tin do một Host gửi đi để truy vấn có router nào đang hoạt động trên cùng phân đoạn mạng. Địa chỉ đích của RA là địa chỉ Multicast ff02::2, đại diện cho tất cả các router ở phạm vi Link.

Router Advertisement (RA):

Bản tin này do router phản hồi lại bản tin RS hoặc có thể router tự quảng bá định kỳ cho các Host biết. Nếu là bản tin phản hồi cho bản tin RS thì địa chỉ đích của bản tin RA là địa chỉ của Host đã gửi truy vấn còn nếu là bản tin RS tự gửi định kỳ thì đích sẽ là ff02::1, địa chỉ đại diện cho tất cả các node mạng ở phạm vi Link hay còn gọi là địa chỉ Broadcast.



Hình 70. Hoạt động của Router Solicitation và Router Advertisement

Neighbor Solicitation (NS):

Cũng giống như ARP Request, bản tin NS nhằm truy vấn địa chỉ MAC cho một địa chỉ IPv6 gửi đến các Neighbor trên cùng lớp mạng. Bản tin này còn được dùng để kiểm trùng địa chỉ IPv6. Trong trường hợp để phân giải địa chỉ MAC thì địa chỉ nguồn của bản tin NS là địa chỉ của thiết bị khởi tạo bản tin và địa chỉ đích là địa chỉ Solicited Node Multicast. Nếu mục đích là nhằm kiểm tra một địa chỉ có bị trùng thì địa chỉ nguồn của bản tin NS là địa chỉ IPv6 đặc biệt Unspecified Unicast ::/128 và địa chỉ đích là địa chỉ cần kiểm tra.

Neighbor Advertisement (NA):

Giống ARP Response, các Neighbor gửi phản hồi lại địa chỉ MAC của mình tương ứng với địa chỉ IPv6 trong bản tin NS nhận được. Lúc đó địa chỉ đích của bản tin NA sẽ là địa chỉ nguồn của bản tin NS. Trường hợp bản tin NA phản hồi lại cho việc kiểm trùng thì đích của NA là địa chỉ Broadcast **ff02::1**.

Đôi khi các thiết bị cũng tự động gửi các bản tin NA mà không cần nhận được bản tin NS trước đó. Tình huống này xảy ra khi các thiết bị thay đổi địa chỉ MAC hay IPv6 và muốn cập nhật thông tin cho các thiết bị khác. Địa chỉ đích của bản tinh NA trường hợp này cũng là **ff02::1**.

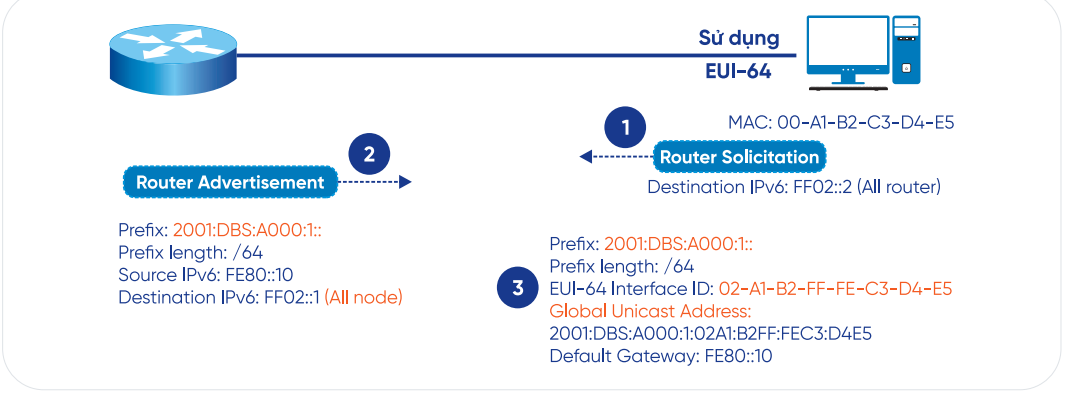
Hình 71. Hoạt động của Neighbor Solicitation và Neighbor Advertisement

Redirect Message:

Giống với bản tin Redirect của ICMP trong IPv4, dùng để đổi Next-hop tối ưu hơn cho Host nhưng ít được dùng thực tế.

4.8. KỸ THUẬT GÁN ĐỊA CHỈ TỰ ĐỘNG SLAAC

SLAAC (Stateless Address Autoconfiguration) là tính năng mới và khá quan trọng của IPv6, cho phép các thiết bị tự động tạo và gán địa chỉ IPv6 mà không cần đến máy chủ DHCP. Khi kết nối vào mạng, thiết bị sẽ nhận thông tin từ các router trong mạng và tự động cấu hình địa chỉ IPv6 cho mình. SLAAC giúp đơn giản hóa quá trình khai báo địa chỉ mạng, đặc biệt hữu ích trong các hệ thống mạng lớn như 5G và IoT. Tính tự động này của SLAAC giúp tiết kiệm thời gian và công sức hơn so với việc sử dụng DHCP Server nên mang lại sự linh hoạt và hiệu quả cho mạng IPv6.



Hình 72. Chi tiết hoạt động của SLAAC

Hoạt động của SLAAC dựa vào hai bản tin chính của NDP là Router Solicitation (RS) và Router Advertisement (RA) được mô tả ở trên. Quá trình một máy tính tự gán địa chỉ IPv6 cho chính mình sẽ bao gồm các bước như sau:

Tạo địa chỉ Link-Local:

Máy tính tự động tạo một địa chỉ Link-Local ngẫu nhiên, ví dụ như fe80::d0f8:9ff6:4201:7086 trong hình trên, làm địa chỉ nguồn để giao tiếp với các router trong mạng cục bộ. Thay vì sử dụng bản tin Layer 2, vốn thường được truyền quảng bá (Broadcast) như của DHCPv4, thì với địa chỉ IPv6 Link-Local trên, các bản tin sẽ được gửi đến địa chỉ nhóm Solicited-Node Multicast. Với cách này các bản tin chỉ được gửi đến các thiết bị liên quan, giúp tối ưu và giảm tải cho mạng. Địa chỉ Link-Local này được kiểm trùng trước khi được sử dụng (kỹ thuật kiểm trùng sẽ trình bày sau, phần này tập trung vào kỹ thuật SLAAC).

Gửi bản tin RS:

Máy tính gửi bản tin RS có địa chỉ nguồn Link-Local đến địa chỉ Multicast ff02::2, là địa chỉ dành riêng cho các router nên chỉ các router mới tiếp nhận và xử lý bản tin.

Gửi bản tin RA:

Sau khi nhận bản tin RS thì router phản hồi bằng bản tin RA, với nguồn là địa chỉ Link-Local của router và đích là địa chỉ Multicast ff02::1 đại diện cho tất cả các thiết bị mạng (tương đương với địa chỉ Broadcast của IPv4). Một thông tin quan trọng trong RA đó Prefix và Prefix-Length của địa chỉ Unicast (Global hoặc Unique Local) của router (chính xác là của cổng mạng nhận được bản tin RS). Ở ví dụ trên là Prefix 2001:db8:cafe:1:: và Prefix-length /64.

Tạo địa chỉ IPv6 Unicast:

Sau khi nhận được bản tin RA, máy tính sẽ tạo mã định danh giao diện (Interface-ID) kết hợp với Prefix từ bản tin RA để thành địa chỉ IPv6 Unicast đầy đủ dài 128 bit. Địa chỉ này chắc chắn nằm cùng lớp mạng với router và được kiểm trùng trước khi sử dụng (sẽ được trình bày ở phần sau).

Cấu hình Default Gateway:

Máy tính chọn địa chỉ Link-Local của router làm Default Gateway và hoàn tất quá trình tự cấu hình.

Trên đây là những bước chính mô tả hoạt động của kỹ thuật **SLAAC**. Thông qua các bản tin **Router Solicitation (RS) và Router Advertisement (RA)**, các thiết bị có thể tự động sinh địa chỉ IPv6 cho riêng mình mà không phụ thuộc vào máy chủ DHCP. Ở bước 4, việc tạo **Interface-ID** có thể dựa trên địa chỉ MAC hoặc sử dụng phương pháp sinh địa chỉ ngẫu nhiên, chi tiết sẽ được trình bày ở phần sau.

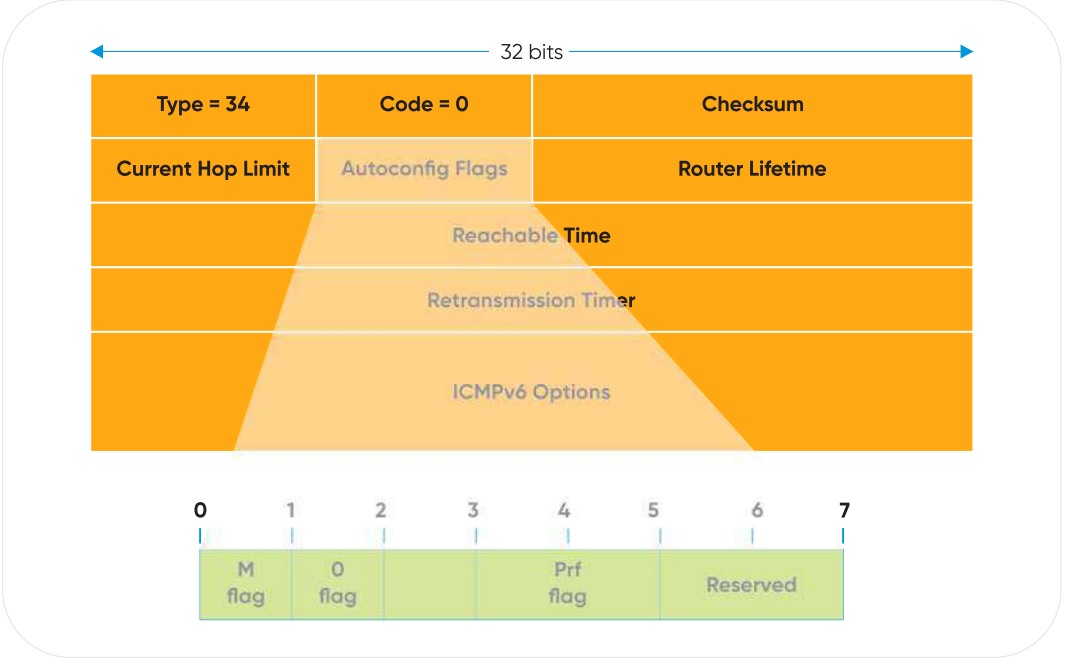
Tuy nhiên, cần lưu ý rằng SLAAC chỉ cung cấp địa chỉ IPv6 và **Default Gateway**, nhưng không bao gồm thông tin về **DNS Server**. Do đó, kỹ thuật này chưa đủ để đảm bảo thiết bị truy cập Internet mà cần kết hợp với các phương pháp khác hoặc sử dụng **DHCPv6**. Để giải quyết hạn chế này, **RFC 8106** đã giới thiệu một tùy chọn cho phép router cung cấp địa chỉ DNS thông qua bản tin RA, thay vì phụ thuộc vào DHCPv6. Tính năng này, được gọi là **RDNSS (Recursive DNS Server)**, đã được một số nhà sản xuất thiết bị tích hợp và hỗ trợ, nâng cao tính hiệu quả của SLAAC.

```
R1# show ipv6 interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es)
Global unicast address(es):
  2001:DB8:CAFE:1::1, subnet is 2001:DB8:CAFE:1::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::FB
  FF02::1:FF00:1

**MTU is 1500 bytes**

ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent

ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)

**ND router advertisements are sent every 200 seconds**
**ND router advertisements live for 1800 seconds**
**ND advertised default router preference is Medium**
**Hosts use stateless autoconfig for addresses.**
```

Hình 73. Thông tin về giao thức NDP và SLAAC trên cổng router

4.9. STATELESS DHCPv6

Kỹ thuật SLAAC được gọi là Stateless (không trạng thái) vì không cần thiết bị nào lưu thông tin, địa chỉ IPv6 được gán tự động cho các thiết bị giống như trường hợp sử dụng DHCPv6 Server. Tuy nhiên, SLAAC chủ yếu tạo và gán IPv6 tự động chứ không cung cấp các thông tin khác như DNS hoặc một số tùy chọn như đối với DHCPv6. Chính vì thế SLAAC có thể được sử dụng kết hợp với DHCPv6, lúc này SLAAC được dùng để cung cấp địa chỉ IPv6 và Default Gateway trong khi DHCPv6 được sử dụng để cấp các thông tin khác. Mô hình này được gọi là "Stateless DHCPv6", để phân biệt với "Stateful DHCPv6" truyền thống, trong đó DHCPv6 sẽ đảm nhận toàn bộ quá trình cấu hình địa chỉ IPv6 cho các thiết bị.



Hình 74. Cấu trúc bản tin Router Advertisement

Trong cấu trúc của bản tin RA (Router Advertisement) có một phần gọi là Autoconfiguration Flags đóng vai trò quyết định cách thức cấu hình địa chỉ IPv6 và các thông tin liên quan. Phần này chứa hai bit quan trọng là M Flag (Managed Address Configuration flag) và O Flag (Other Configuration flag), với quy định cụ thể như sau:

Nếu bit O và M đều bằng 0:

Router chỉ cung cấp hai thông tin cơ bản là địa chỉ IPv6 và Default Gateway, các thông tin khác không được cung cấp. Trường hợp này tương ứng với cơ chế SLAAC.

Nếu bit O=1:

Thì router cung cấp địa chỉ IPv6 và Default Gateway còn DHCPv6 sẽ cung cấp các thông tin khác. Đây là trường hợp của Stateless DHCPv6.

Nếu bit M=1:

Thì router chỉ cung cấp địa chỉ Default Gateway còn địa chỉ IPv6 và các thông tin khác đều được cấp bởi DHCPv6 Server. Lúc này giá trị của bit O sẽ không được xét đến. Phương thức này được gọi là Stateful DHCPv6.

```
Router1#show ipv6 interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:1234:A:B::1, subnet is 2001:1234:A:B::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
  Hosts use DHCP to obtain other configuration.
```

Hình 75. Trạng thái của Interface khi khai báo Stateless DHCP

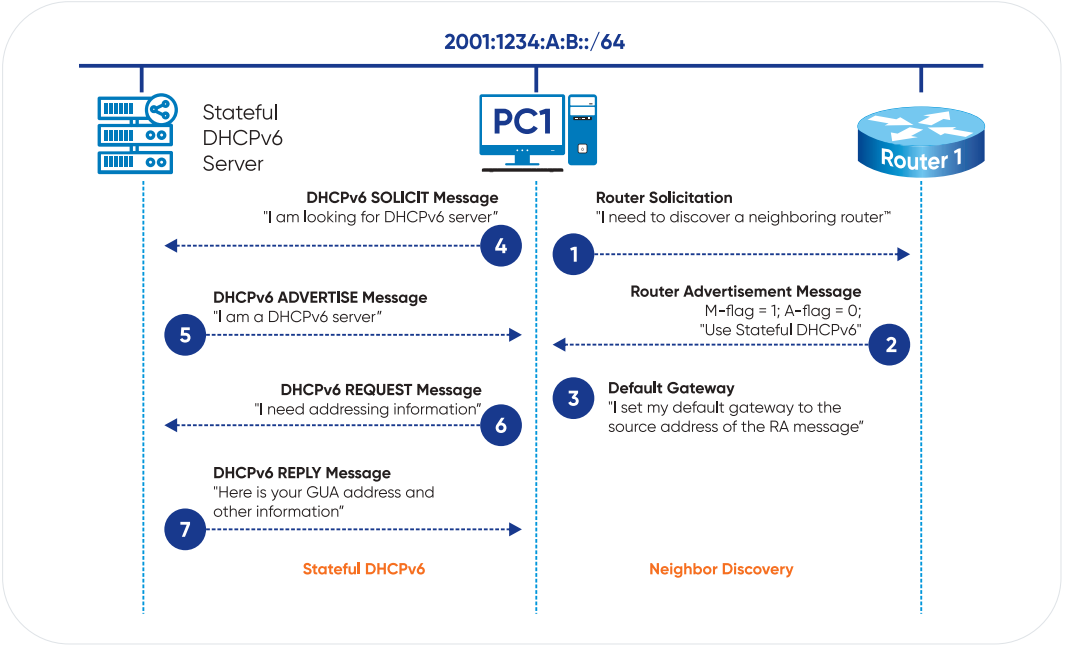
Như vậy, đối với IPv6 chúng ta có nhiều cách khai báo địa chỉ IPv6 và các thông tin liên quan. SLAAC là cơ chế mới so với IPv4 và các thông số M Flag và O Flag của bản tin RA giúp việc kết hợp giữa SLAAC và DHCP trở nên linh hoạt hơn.

Chú ý:

- Một điểm cần lưu ý là dù sử dụng Stateless DHCP hay Stateful DHCP thì bản tin RA vẫn đóng vai trò trong việc xác định địa chỉ Default Gateway, cụ thể là địa chỉ Link-Local của router, cho các thiết bị mạng. Vì vậy, chúng ta không nên vô hiệu hóa việc quảng bá các bản tin này.

4.10. STATEFUL DHCPV6

DHCPv6 kế thừa ý tưởng từ DHCPv4 nhưng đã được tối ưu và mở rộng để phù hợp với các đặc điểm của IPv6. Các bản tin của DHCPv4 như Discover, Offer, Request và Acknowledge được thay thế bằng các bản tin tương ứng trong DHCPv6 là Solicit, Advertise, Request và Reply. Ngoài bốn bản tin chính trên còn có một số bản tin DHCPv6 khác như Renew, Rebind, Release, Decline ... Một điểm khác biệt quan trọng là trong khi DHCPv4 sử dụng địa chỉ Broadcast để trao đổi các bản tin còn DHCPv6 sử dụng địa chỉ Multicast, nên việc truyền các bản tin sẽ tối ưu hơn. DHCPv6 dù hoạt động theo chế độ Stateful nhưng router vẫn tham gia vào quá trình trao đổi giữa Client và DHCPv6 Server, thông qua các bản tin RS và RA, giúp điều phối việc cấu hình mạng.



Hình 76. Chi tiết hoạt động của Stateful DHCPv6

Quá trình cấp phát địa chỉ IPv6 theo mô hình Stateful DHCPv6 gồm những bước chính sau:

Solicit:

Khi một thiết bị kết nối vào mạng, nó gửi bản tin Solicit tới địa chỉ Multicast FF02::1:2, đại diện cho tất cả các DHCPv6 Server trên cùng Link.

Advertise:

Các DHCPv6 Server sau khi nhận bản tin Solicit sẽ phản hồi lại bằng bản tin Advertise, chứa thông số mà các DHCPv6 Server có thể cung cấp. Đây là bản tin Unicast với đích là địa chỉ Link-Local của Client (được gán bằng tay hoặc sinh ra tự động).

Request:

Thiết bị Client sẽ chọn một DHCPv6 Server và gửi bản tin Request để yêu cầu cấp phát địa chỉ IPv6 cùng với các thông số cấu hình mạng như: DNS, Default Gateway, thời gian cho thuê địa chỉ và các tham số khác. Bản tin này cũng là Unicast và có đích là địa chỉ của DHCPv6 được chọn.

Reply:

DHCPv6 Server gửi bản tin Unicast là Reply về cho Client, cấp phát địa chỉ IPv6 và các thông số khác đi kèm. Client sau khi nhận được địa chỉ IPv6 và các thông tin sẽ thực hiện kiểm trùng địa chỉ.

Để lưu thông tin cấp phát cho các Client thì Stateful DHCPv6 cần có định danh cho các Client. Không như DHCPv4 sử dụng địa chỉ MAC để định danh cho Client, với DHCPv6 có nhiều cách để định danh hơn. Hai phương thức định danh chính cho DHCPv6 Client là DUID (DHCP Unique Identifier) và IAID (Identity Association Identifier). Riêng DUID lại có tới bốn kiểu định danh khác nhau gồm:

DUID-LL (Link-Layer): DUID này chỉ sử dụng địa chỉ MAC của Client.

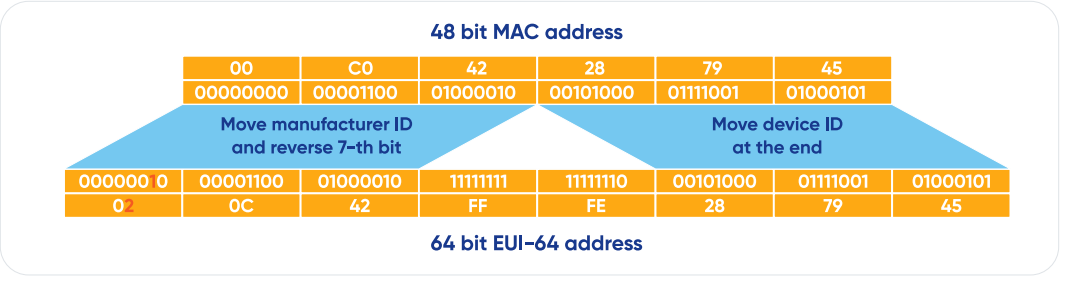
DUID-LLT (Link-Layer + Time): Bao gồm địa chỉ MAC của Client và mốc thời gian tạo DUID.

DUID-EN (Enterprise Number): Sử dụng mã số doanh nghiệp (doanh nghiệp ID) theo chuẩn của IANA (Internet Assigned Numbers Authority) cấp cho các nhà sản xuất thiết bị (Vendor).

Về cơ bản, Stateful DHCPv6 có cách thức hoạt động và tính năng khá giống với DHCPv4 nhưng đã được cải tiến, tối ưu hoạt động và bổ sung thêm các tính năng thông qua các bản tin mới.

4.11. EUI-64 TẠO INTERFACE-ID THEO ĐỊA CHỈ MAC

Với kỹ thuật SLAAC, các thiết bị mạng sau khi nhận được Prefix và Prefix Length thông qua bản tin, RA sẽ tự tạo cho mình định danh giao diện (Interface-ID) nhằm kết hợp với Prefix để tạo thành một địa chỉ IPv6. Để đảm bảo tính duy nhất cho địa chỉ IPv6 này thì có một phương án là sử dụng địa chỉ MAC của thiết bị để tạo Interface-ID. Tuy nhiên địa chỉ MAC chỉ có 48 bit trong khi Interface-ID là 64 bit nên không thể sử dụng trực tiếp địa chỉ MAC mà cần có một nguyên tắc và đó là nguyên tắc có tên gọi **EUI-64 (Extended Unique Identifier)**.



Hình 77. Chi tiết nguyên tắc của EUI-64

Mỗi địa chỉ MAC 48 bit gồm có 2 phần, mỗi phần đều có 24 bit: **Organizationally Unique Identifier (OUI)** đại diện cho nhà sản xuất thiết bị và **Device ID** định danh cho mỗi thiết bị của nhà sản xuất đó. Giá trị OUI là duy nhất vì được quản lý và cấp phát bởi IEEE và mỗi nhà sản xuất phải tạo ra định danh duy nhất cho mỗi thiết bị mạng của mình nên địa chỉ MAC của mỗi thiết bị sẽ là duy nhất. Chính tính duy nhất này đã sinh ra kỹ thuật EUI-64 với nguyên tắc chuyển đổi từ 48 bit sang 64 bit như sau:

Tách OUI và Device ID:

Phần OUI và định danh thiết bị được tách riêng. Trong OUI, có một bit tham dự vào nguyên tắc EUI-64 đó là bit thứ 7 với tên gọi là Universal/Local (U/L) bit. Nếu U/L bit = 0, địa chỉ MAC được nhà sản xuất gán và mang tính toàn cầu. Nếu U/L bit = 1, địa chỉ MAC được tự tạo bởi người dùng, ví dụ để gán cho Serial hoặc Tunnel Interface, nhằm phân biệt với địa chỉ từ nhà sản xuất.

Thêm 16 bit mã FFFE:

Một chuỗi 16 bit (giá trị Hexa FFFE, tương ứng với hệ nhị phân 1111 1111 1111 1110) được chèn vào giữa hai phần OUI và Device ID.

Đảo giá trị U/L bit:

Bit số 7 U/L sẽ bị đảo ngược từ 0 sang 1.

Tạo mã định danh 64 bit:

Kết hợp các bước trên, địa chỉ MAC 48 bit được chuyển thành định danh 64 bit và khả năng định danh này bị trùng rất thấp.

Tạo địa chỉ IPv6:

Mã định danh 64 bit được ghép với Prefix /64 nhận từ bản tin RA, tạo ra địa chỉ IPv6 duy nhất, phục vụ cho kỹ thuật SLAAC.

Kỹ thuật EUI-64 giúp tự động tạo địa chỉ IPv6 duy nhất từ địa chỉ MAC 48 bit, đơn giản hóa quá trình cấu hình trong SLAAC. Nó sử dụng OUI và Device ID, kết hợp với mã FFFE và đảo ngược bit thứ 7, để tạo Interface-ID 64 bit. Thông qua đó, các thiết bị mạng có thể tự động cấu hình địa chỉ IPv6 mà không cần khai báo thủ công hoặc sử dụng DHCPv6, giúp tiết kiệm thời gian và đơn giản trong quản lý.

Chú ý:

- Kỹ thuật EUI-64 có thể áp dụng cho cả địa chỉ Global Unicast, Unique Local và Link Local.
- Việc đảo ngược bit thứ 7 của OUI trong kỹ thuật EUI-64 vẫn đang có nhiều ý kiến vì chưa giải thích rõ lợi ích của việc chuyển đổi này.
- Nếu bit số 7 ban đầu đang bằng 1 thì vẫn bị đảo ngược thành 0.

4.12. RFC 4941 TẠO INTERFACE-ID NGẪU NHIÊN

Việc sử dụng kỹ thuật EUI-64 rất đơn giản nhưng bảo đảm tính duy nhất cho địa chỉ IPv6 được tạo ra nhưng cũng kéo theo vấn đề liên quan đến bảo mật và riêng tư.

Rủi ro bị tấn công:

Nếu kẻ tấn công biết địa chỉ MAC của một thiết bị thì sẽ dễ dàng dò ra được địa chỉ IPv6 của thiết bị đó và từ đó dễ dàng theo dõi và tấn công vào địa chỉ IPv6 đích.

Vấn đề về quyền riêng tư:

Vì địa chỉ IPv6 được tạo từ địa chỉ MAC nên một thiết bị dù di chuyển sang bất kỳ mạng nào cũng dễ bị đoán và bị theo dõi.

Để bảo vệ quyền riêng tư và giảm thiểu rủi ro tấn công, RFC 4941 đã đề xuất sử dụng địa chỉ IPv6 ngẫu nhiên thay vì sử dụng EUI-64, cụ thể như sau:

Tạo Interface ID ngẫu nhiên:

Thay vì sử dụng địa chỉ MAC (EUI-64) để tạo địa chỉ, RFC 4941 cho phép tạo địa chỉ ngẫu nhiên cho Interface ID. Việc này giúp dấu thông tin của thiết bị, giảm thiểu khả năng bị theo dõi giúp bảo vệ quyền riêng tư cho người dùng.

Tạo thêm địa chỉ tạm thời (Temporary Address):

Ngoài địa chỉ IPv6 chính được tạo ra với Interface-ID ngẫu nhiên, RFC 4941 cũng đề xuất tạo thêm một địa chỉ nữa gọi là địa chỉ tạm thời. Địa chỉ này cũng có Interface-ID ngẫu nhiên nhưng có thời gian tồn tại ngắn hơn địa chỉ chính. Địa chỉ chính được dùng cho trao đổi dữ liệu nội bộ, còn địa chỉ tạm thời được dùng cho các kết nối ra bên ngoài Internet.

```
C:\Windows\system32>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix . :
   IPub Address ..........: fdbe:6442:2ece:0:80ac:4cb2:3528:ebb
   Temporary IPv6 Address.....: fdbe:6442:2ece:0:1d2e:9451:dc43:665c
   Link-local IPub Hddress.....: fe80::80ac:4cb7:3578:ebb%11
   Default Gateway.....: fe80::ca00:cff:fe34:0%11

C:\Windows\system32>
```

Hình 78. Địa chỉ IPv6 chính và tạm thời

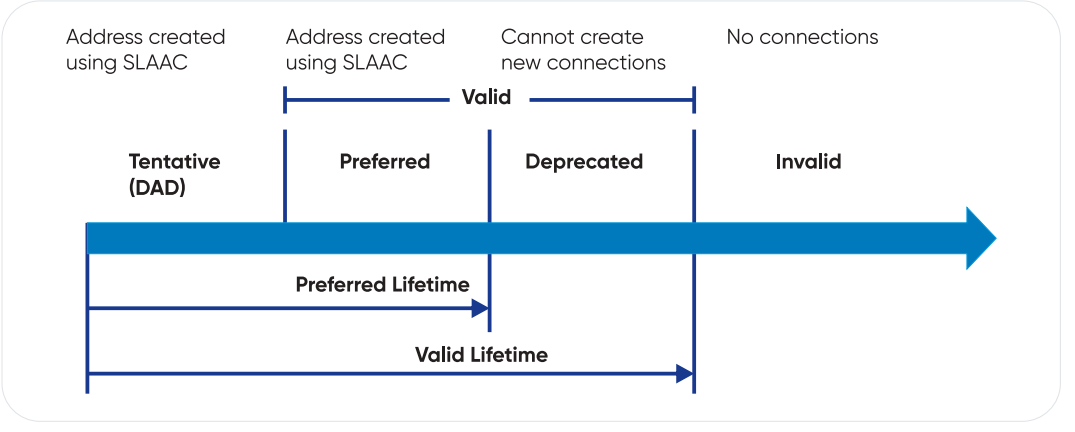
RFC 4941 là một bước tiến quan trọng trong việc bảo vệ quyền riêng tư và nâng cao bảo mật cho người dùng và làm cho IPv6 phù hợp hơn với các yêu cầu bảo mật trong môi trường hiện đại. Hiện nay các hệ điều hành phổ biến như Windows, MAC, Linux đã hỗ trợ RFC 4941 này.

Chú ý:

- Trong thực tế có trường hợp một máy tính có một địa chỉ chính nhưng rất nhiều địa chỉ Temporary. Bình thường địa chỉ Temporary sẽ bị mất đi sau một khoảng thời gian quy định (Valid time) và sau đó một địa chỉ Temporary mới được sinh ra. Sau thời gian Valid time, nếu vẫn có một phiên kết nối đang sử dụng địa chỉ Temporary cũ thì địa chỉ này sẽ tiếp tục tồn tại tới khi phiên kết nối đó kết thúc.

4.13. CÁC TRẠNG THÁI HOẠT ĐỘNG CỦA ĐỊA CHỈ IPv6

Các địa chỉ IPv6 nhận động dù qua SLAAC, Stateless hoặc Stateful đều có một khoảng thời gian hữu hiệu và trải qua các trạng thái hoạt động khác nhau. Dưới đây là những trạng thái hoạt động của địa chỉ IPv6:



Hình 79. Các trạng thái của địa chỉ IPv6

Địa chỉ dự kiến (Tentative address):

Một địa chỉ IPv6 sau khi được cấp động hoặc khai báo thủ công sẽ không được sử dụng ngay mà cần phải được kiểm trùng, nên đây là địa chỉ dự kiến. Những gói tin gửi đến địa chỉ dự kiến này sẽ bị loại bỏ trừ những bản tin NDP liên quan đến việc kiểm trùng.

Địa chỉ hợp lệ (Valid address):

Mỗi địa chỉ IPv6 cấp động được phép hoạt động trong khoảng thời gian cho phép (Valid time), trong thời gian này địa chỉ được coi là hợp lệ. Địa chỉ hợp lệ được phân thành hai loại nữa là **Preferred** và **Deprecated**. Thời gian Valid time này được router thông báo qua bản tin RA.

Địa chỉ ưu tiên (Preferred address):

Ngay sau khi được kiểm trùng thì địa chỉ IPv6 được ưu tiên sử dụng để thiết lập các kết nối. Thời gian địa chỉ ở trạng thái ưu tiên (Preferred time) cũng được router thông báo qua bản tin router Advertisement. Yêu cầu thời gian Preferred time phải nhỏ hơn hoặc bằng Valid time.

Địa chỉ hết hiệu lực (Deprecated address):

Sau thời gian Preferred time địa chỉ IPv6 sẽ chuyển sang trạng thái hết hiệu lực và một địa chỉ IPv6 mới được tạo ra. Dù vẫn được xem là hợp lệ nhưng địa chỉ Deprecated này không được sử dụng để tạo các kết nối mới mà chỉ để duy trì cho các kết nối đang hoạt động vì nếu chuyển kết nối đang hoạt động sang địa chỉ IPv6 mới thì sẽ làm gián đoạn hoạt động của lớp trên.

Địa chỉ không hợp lệ (Invalid address):

Sau thời gian Deprecated time, địa chỉ IPv6 sẽ trở thành không hợp lệ và tất cả các kết nối đi từ hoặc đi đến địa chỉ này đều không được phép.

Trạng thái Deprecated nhằm thông báo cho các lớp trên của tầng mạng ưu tiên sử dụng địa chỉ IPv6 Prefered mới thay vì địa chỉ Deprecated để tránh tình trạng kết nối bị gián đoạn khi hết thời gian hợp lệ.

4.14. KỸ THUẬT PHÂN GIẢI ĐỊA CHỈ MAC

Đối với IPv4, giao thức ARP được dùng để phân giải địa chỉ MAC tương ứng với địa chỉ IPv4 thông qua việc Broadcast các bản tin. Giao thức NDP đã thay thế cho ARP, giúp việc phân giải địa chỉ MAC cho địa chỉ IPv6 tối ưu hơn vì NDP sử dụng nhóm Multicast thay cho Broadcast. Hai bản tin quan trọng của NDP phục vụ cho việc phân giải này là Neighbor Solicitation (NS) và Neighbor Advertisement (NA). Việc phân giải này được gọi là Neighbor Discovery.

ICMP Type	135 NS	ICMP Type	136 NA
IPv6 Source	fe80::a	**IPv6 Source**	fe80::b
IPv6 Destination	ff02::1:ff00:b	**IPv6 Destination**	fe80::a
Hop Limit	255	Target Address	2001:db8:1:46::b
Target Address	2001:db8:1:46::b	**Option 2 TLLA**	**B's Link Layer Address**
Query	What is B link layer address?	***Flags**	R = Router S = Response to Solicitation O = Override cache information
Opt. 1 SLLA	A's Link Layer Address		

Hình 80. Các bản tin trong kỹ thuật phân giải địa chỉ MAC và IPv6

Chi tiết quá trình phân giải địa chỉ MAC từ địa chỉ IPv6 như sau:

Bước 1: Kiểm tra Neighbor Cache

Thiết bị gửi gói tin kiểm tra thông tin lưu trữ (Neighbor Cache) để tìm địa chỉ MAC tương ứng với địa chỉ IPv6 đích. Nếu có thì sẽ dụng địa chỉ MAC này, còn không thì sẽ gửi bản tin Neighbor Solicitation (NS) để bắt đầu quá trình phân giải địa chỉ.

Bước 2: Gửi bản tin Neighbor Solicitation (NS)

Thiết bị gửi bản tin NS đến các thiết bị khác trên cùng phân đoạn mạng, bản tin này có đặc điểm sau:

- Địa chỉ đích: Là **Solicited-Node Multicast** của địa chỉ IPv6 Unicast cần được phân giải thay vì dùng Broadcast như đối với ARP.
- Trường **Hop Limit** trong tiêu đề IPv6 của bản tin NS được đặt giá trị 255 nhằm đảm bảo bản tin xuất phát từ phân đoạn mạng cục bộ (link-local) để ngăn chặn các bản tin giả mạo gửi từ mạng khác tới.

Bước 3: Nhận và kiểm tra bản tin NS

Thiết bị đích nhận bản tin NS và kiểm tra giá trị Hop Limit nếu không phải là 255 thì bản tin bị loại bỏ, trường hợp là 255 thì thiết bị đích chuẩn bị bản tin Neighbor Advertisement (NA) để phản hồi.

Bước 4: Gửi Neighbor Advertisement (NA)

Thiết bị đích gửi phản hồi bản tin NA trở lại thiết bị nguồn chứa thông tin địa chỉ IPv6 và địa chỉ MAC tương ứng. Bản tin này là bản tin Unicast vì địa chỉ nguồn và địa chỉ đích đã rõ ràng.

Bước 5: Cập nhật Neighbor Cache

Thiết bị nguồn nhận thông điệp NA, cập nhật **Neighbor Cache** với ánh xạ thông tin địa chỉ IPv6 và địa chỉ MAC nhận được.

Có thể thấy hoạt động của NDP tối ưu hơn nhiều so với ARP do sử dụng địa chỉ Multicast thay cho Broadcast, ngoài ra việc yêu cầu Hop limit = 255 cũng là cơ chế giúp phòng chống tấn công giả mạo địa chỉ từ mạng bên ngoài.

4.15. CÁC TRẠNG THÁI TRONG NEIGHBOR CACHE

Sau khi được phân giải, thông tin ánh xạ giữa địa chỉ IPv6 và MAC sẽ được lưu trong bảng Neighbor Cache. Thông tin Neighbor trong bảng này có năm trạng thái như sau:

Incomplete

Đây là trạng thái đầu tiên khi thiết bị tiến hành phân giải địa chỉ MAC, lúc này bản tin Neighbor Solicitation (NS) đã được gửi đi nhưng chưa nhận được bản tin phản hồi Neighbor Advertisement (NA). Nếu sau 3 lần gửi thông điệp NS mà không nhận được phản hồi NA, thì địa chỉ IPv6 sẽ bị xóa khỏi bảng Neighbor Cache.

Reachable

Tại trạng thái này, thiết bị đã nhận được thông tin địa chỉ MAC tương ứng với địa chỉ IPv6 của Neighbor và sẵn sàng cho việc trao đổi thông tin.

Stale

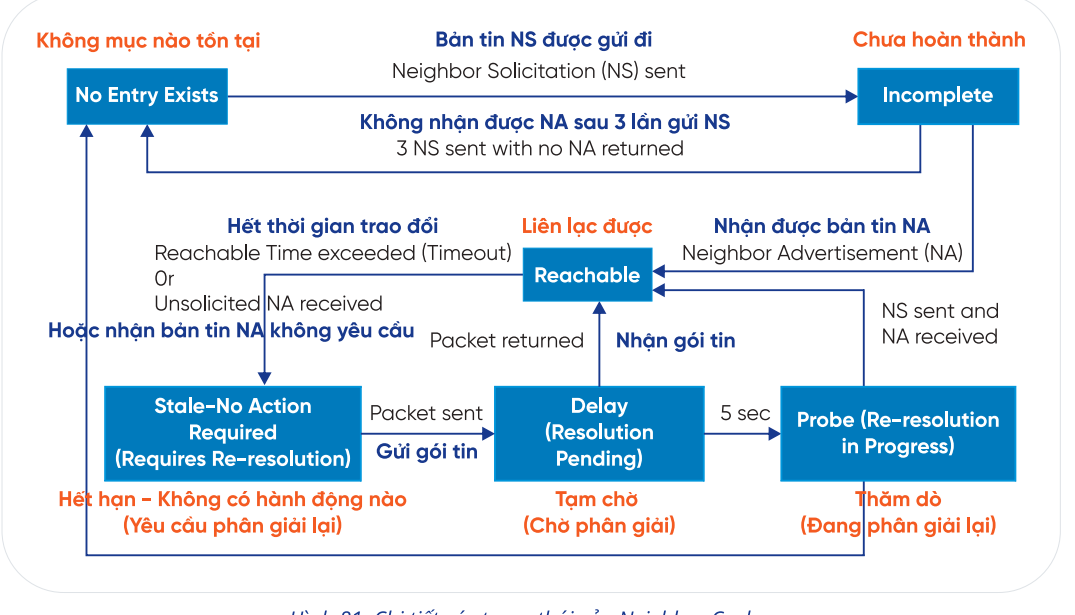
Khi chuyển sang trạng thái Reachable thì một khoảng thời gian thiết lập gọi là Reachable Time (giống Aging Time của ARP). Sau thời gian này nếu thiết bị không nhận được bất kỳ gói tin nào từ Neighbor thì địa chỉ IPv6 sẽ chuyển sang trạng thái Stale.

Delay

Sau khi chuyển sang Stale nếu thiết bị nhận được yêu cầu truyền dữ liệu đến Neighbor từ các tầng ở trên (ví dụ, gói tin TCP Syn) thì địa chỉ IPv6 của Neighbor được chuyển sang trạng thái Delay. Khi đó thiết bị vẫn sử dụng thông tin địa chỉ MAC cũ và tiếp tục gửi bản tin từ tầng trên đến đích mà không cần thăm dò lại bằng bảng tin NS. Nếu trong vòng 5 giây, thiết bị nhận lại thông tin phản hồi (ví dụ như TCP Syn/Ack) thì địa chỉ IPv6 của Neighbor chuyển sang trạng thái **Reachable**. Ngược lại, nếu không nhận được phản hồi, trạng thái của địa chỉ IPv6 sẽ chuyển sang **Probe** để thăm dò lại.

Probe

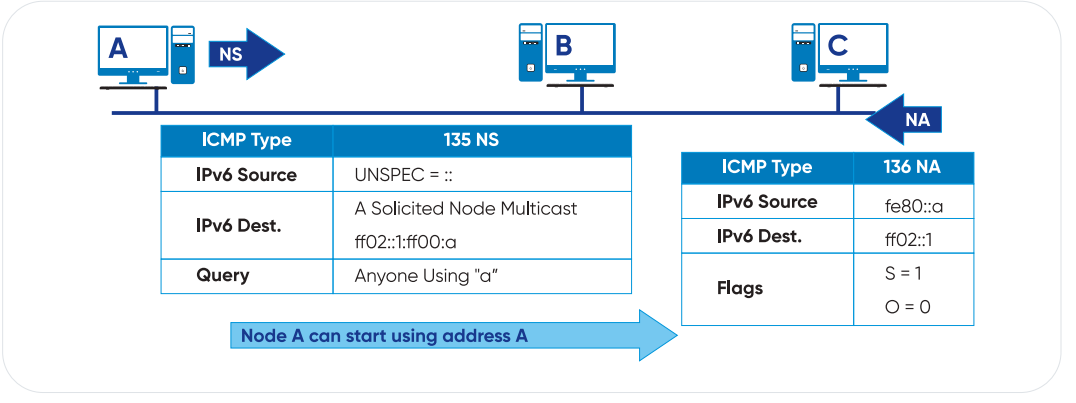
Ở trạng thái này thiết bị sẽ gửi bản tin NS để yêu cầu lại địa chỉ MAC. Nếu nhận được phản hồi thông qua bản tin NA thì trạng thái sẽ trở về Reachable, còn nếu gửi NS 3 lần mà không nhận được phản hồi thì địa chỉ IPv6 của Neighbor bị xóa khỏi bảng Neighbor Cache.



Hình 81. Chi tiết các trạng thái của Neighbor Cache

4.16. KỸ THUẬT KIỂM TRÙNG ĐỊA CHỈ DAD

Khi một thiết bị được khai báo địa chỉ IPv6 thủ công hoặc nhận tự động thì địa chỉ đó sẽ không được sử dụng ngay mà cần phải trải qua quá trình kiểm trùng Duplicate Address Detection (DAD) để bảo đảm địa chỉ đó là duy nhất. Địa chỉ cần kiểm trùng là bất kỳ địa chỉ Unicast nào như Link Local, Unique Local hoặc Global Unicast.



Hình 82. Các bản tin trong kỹ thuật phân kiểm trùng địa chỉ

Chi tiết quá trình kiểm trùng địa chỉ DAD bao gồm những bước sau:

Bước 1: Tạo địa chỉ IPv6 dự kiến

Khi một địa chỉ IPv6 được khai báo hoặc gán tự động, nó sẽ được xem là địa chỉ dự kiến (Tentative IPv6 address) và chưa được sử dụng cho đến khi quá trình kiểm tra DAD hoàn tất.

Bước 2: Gửi Neighbor Solicitation (NS)

Thiết bị sẽ gửi một bản tin Neighbor Solicitation (NS) với địa chỉ nguồn là :: (Unspecified Unicast), đại diện cho 128 bit số 0, vì lúc này địa chỉ IPv6 Unicast được gán chưa thể sử dụng. Địa chỉ đích của bản tin NS là Solicited-node Multicast tương ứng với địa chỉ IPv6 đang cần được kiểm tra. Phần nội dung bản tin NS chứa địa chỉ IPv6 cần kiểm tra.

Bước 3: Kiểm tra kết quả

Sau khi gửi đi bản tin NS, nếu thiết bị gửi không nhận được phản hồi NA sau một khoảng thời gian xác định thì có nghĩa không có một địa chỉ nào tương tự trên mạng, lúc này địa chỉ dự kiến sẽ được sử dụng để giao tiếp và trao đổi dữ liệu với các thiết bị khác. Trong trường hợp nhận được phản hồi NA, có nghĩa địa chỉ IPv6 đã được sử dụng trên mạng nội bộ, lúc này thiết bị sẽ không sử dụng địa chỉ này và có thể thông báo lỗi (nếu gán tĩnh) hoặc tiến hành thủ tục lựa chọn một địa chỉ IPv6 khác.

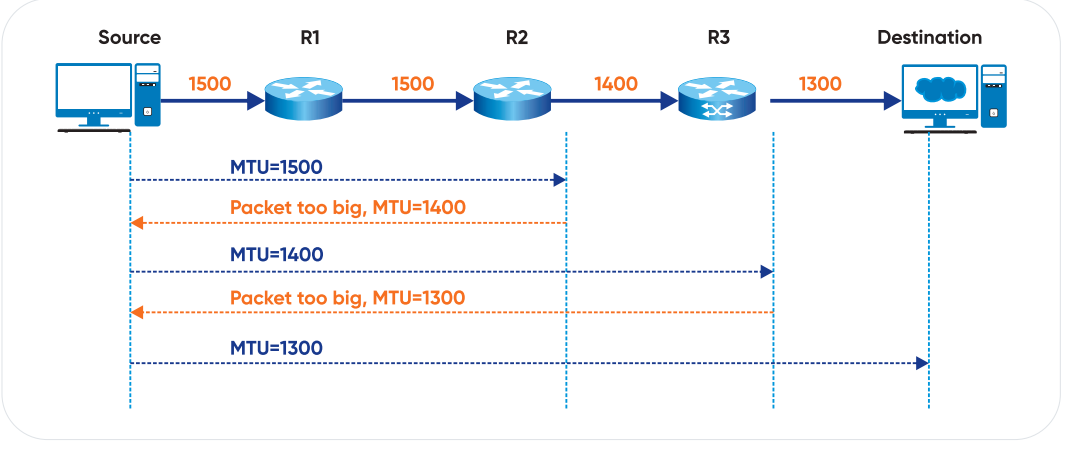
Chú ý:

- Việc kiểm tra trùng sử dụng địa chỉ multicast "Solicited-Node", được tạo từ 24 bit thấp của địa chỉ IPv6 Uncast cần kiểm tra. Vì thế có thể nhiều thiết bị trên cùng một đoạn mạng dùng chung địa chỉ multicast này. Khi một bản tin Neighbor Solicitation (NS) được gửi đi, những thiết bị trên nhận được sẽ kiểm tra nội dung bản tin. Chỉ thiết bị nào đang sử dụng địa chỉ trùng khớp với địa chỉ chứa trong bản tin NS mới phản hồi bằng bản tin Neighbor Advertisement (NA) nhằm thông báo địa chỉ IPv6 cần kiểm đang được sử dụng.

4.17. KỸ THUẬT DÒ TÌM IPv6 PATH MTU (PMTU)

Path MTU Discovery là một kỹ thuật quan trọng giúp tối ưu việc truyền dữ liệu. Trước khi gửi dữ liệu đi, các thiết bị sẽ dò tìm giá trị MTU phù hợp nhất trước khi truyền dữ liệu. Nếu sử dụng MTU nhỏ thì việc truyền sẽ không hiệu quả, nếu dùng MTU lớn thì dẫn đến việc phân mảnh gói tin.

Một bản tin ICMPv6 mới và khá quan trọng đối với quá trình PMTU đó là Packet Too Big (PTB). Khi một thiết bị trung gian nhận thấy gói tin IPv6 lớn hơn giá trị MTU của cổng kết nối cần chuyển gói tin đi thì thiết bị đó sẽ loại bỏ gói tin và tạo ra bản tin Packet Too Big gửi ngược lại cho thiết bị nguồn yêu cầu phân mảnh gói tin. Đây là điều khác biệt rất căn bản so với IPv4 vì các thiết bị trung gian sẽ phân mảnh gói tin IPv4 thay vì thông báo và yêu cầu phân mảnh từ thiết bị nguồn như IPv6. Thông tin quan trọng trong bản tin Packet Too Big đó là giá trị MTU cần điều chỉnh cho phù hợp.



Hình 83. Hoạt động của IPv6 Path MTU

Sau đây là cách hoạt động của Path MTU Discovery:

Bước 1: Khởi tạo và gửi gói tin

Thiết bị nguồn tạo gói tin với giá trị MTU ban đầu, bằng MTU của kết nối từ thiết bị đến router đầu tiên (thường là 1500 byte) và gửi gói tin đi.

Bước 2: Xử lý tại thiết bị trung gian:

Nếu thiết bị mạng trung gian (router) phát hiện kích thước gói tin lớn hơn MTU của cổng nối đến thiết bị kế tiếp, nó sẽ loại bỏ gói tin và gửi thông báo ICMPv6 Packet Too Big về thiết bị nguồn, kèm theo giá trị MTU cần điều chỉnh.

Bước 3: Điều chỉnh kích thước và gửi lại:

Gửi lại gói tin mới với kích thước MTU bằng giá trị trong bản tin ICMPv6 Packet Too Big nhận được. Quá trình này lặp lại nếu tiếp tục nhận thông báo tương tự, cho đến khi gói tin được truyền thành công.

Bước 4: Lưu trữ thông tin MTU cuối cùng

Thiết bị nguồn lưu thông tin MTU cuối cùng tương ứng với địa chỉ IPv6 đích trong bảng MTU Cache.

Hoạt động Path MTU Discovery của IPv6 tương đối giống như IPv4 nhưng sử dụng bản tin khác nhau. Điều khác biệt quan trọng giữa hai giao thức này đó là thiết bị mạng trung gian không thực hiện phân mảnh gói tin có MTU lớn mà thông báo lại bản tin ICMPv6 Packet Too Big cho thiết bị nguồn.

Chú ý:

- Nếu ICMPv6 hoặc bản tin Packet Too Big bị chặn thì việc dò tìm PMTU và việc phân mảnh gói tin không thể thực hiện. Vì thế RFC 4821 đã đưa ra một giải pháp mới có tên "Packetization Layer Path MTU Discovery" (PLPMTUD), giải pháp này không sử dụng ICMPv6 mà sử dụng các giao thức ở lớp trên, ví dụ như TCP. Các giao thức lớp trên sẽ truyền các gói tin với kích thước MTU nhỏ để xem các gói tin có được truyền thành công không, sau đó sẽ nâng dần lên cho đến khi xuất hiện thông báo lỗi. Phương pháp này giúp tránh hiện tượng "Path MTU Black Hole" như đối với IPv4 nên giúp tăng độ tin cậy khi truyền dữ liệu qua mạng.

4.18. TỔNG KẾT CHƯƠNG 4

Trong chương 4, chúng ta đã khám phá vai trò quan trọng của **giao thức ICMPv6** trong hệ thống mạng IPv6, cũng như các kỹ thuật và dịch vụ mạng phổ biến liên quan. Bắt đầu với ICMPv4 và tiến tới tìm hiểu ICMPv6, nội dung của chương trình bày chi tiết về cách thức ICMPv6 hỗ trợ các hoạt động giám sát, chẩn đoán và xử lý sự cố trong mạng, thay thế và tối ưu hóa nhiều chức năng so với IPv4. Bên cạnh đó, chương cũng đã đi sâu vào **Neighbor Discovery Protocol (NDP)**—một giao thức cốt lõi trong IPv6, giúp quản lý quá trình phân giải địa chỉ, tìm kiếm lân cận và tự động gán địa chỉ. Các phương pháp cấp phát địa chỉ như **SLAAC và DHCPv6**, kỹ thuật kiểm tra địa chỉ **DAD** và quy trình **Path MTU Discovery (PMTUD)** cũng được giới thiệu nhằm đảm bảo truyền tải dữ liệu tối ưu trên mạng IPv6. Việc hiểu rõ những nội dung này sẽ giúp bạn vận hành hệ thống mạng IPv6 một cách hiệu quả, tận dụng tối đa lợi thế của các giao thức mới và đảm bảo tính ổn định cũng như hiệu suất của mạng. Đây là nền tảng quan trọng để tiếp tục nghiên cứu các dịch vụ mạng nâng cao và tối ưu hóa hệ thống trong các chương tiếp theo.

4.19. CÂU HỎI ÔN TẬP CHƯƠNG 4

01

Giao thức ICMP có vai trò gì trong mạng và ICMPv6 khác biệt như thế nào so với ICMPv4?

Giao thức ICMP (Internet Control Message Protocol) đóng vai trò quan trọng trong việc hỗ trợ IP bằng cách cung cấp các cơ chế báo lỗi, kiểm tra kết nối và giám sát chất lượng đường truyền. ICMPv6, được phát triển và bổ sung nhiều tính năng so với ICMPv4, trở thành một thành phần cốt lõi trong hầu hết các dịch vụ mạng IPv6. Nó không chỉ thực hiện các chức năng tương tự ICMPv4 một cách hiệu quả hơn mà còn tích hợp các giao thức quan trọng khác như NDP (Neighbor Discovery Protocol) và MLD (Multicast Listener Discovery). ICMPv6 loại bỏ các cơ chế không hiệu quả của IPv4 và mang lại những tính năng mới mạnh mẽ hơn cho việc quản lý và tối ưu hóa mạng IPv6.

02

NDP (Neighbor Discovery Protocol) là gì và nó thay thế giao thức nào trong IPv4?

NDP (Neighbor Discovery Protocol) là một giao thức quan trọng trong IPv6, thay thế cho giao thức ARP (Address Resolution Protocol) trong IPv4. NDP sử dụng các bản tin ICMPv6 để thực hiện nhiều chức năng quan trọng như phân giải địa chỉ IPv6 sang địa chỉ MAC, tìm kiếm các thiết bị lân cận, phát hiện router và tự động cấu hình địa chỉ. NDP hoạt động hiệu quả hơn ARP bằng cách sử dụng các bản tin Multicast thay vì Broadcast và tích hợp thêm các cơ chế bảo mật.

03

SLAAC (Stateless Address Autoconfiguration) hoạt động như thế nào và lợi ích của nó là gì?

SLAAC (Stateless Address Autoconfiguration) là một tính năng cho phép các thiết bị tự động tạo và gán địa chỉ IPv6 mà không cần máy chủ DHCP. Khi một thiết bị kết nối vào mạng IPv6, nó sẽ gửi bản tin Router Solicitation (RS) để yêu cầu thông tin từ router. Router sẽ phản hồi bằng bản tin Router Advertisement (RA), chứa tiền tố mạng (Prefix) và độ dài tiền tố. Thiết bị sau đó kết hợp tiền tố này với một Interface-ID (có thể được tạo theo chuẩn EUI-64 từ địa chỉ MAC hoặc ngẫu nhiên theo RFC 4941) để tạo địa chỉ IPv6 Unicast cho chính nó. SLAAC giúp đơn giản hóa việc cấu hình địa chỉ, đặc biệt hữu ích trong các mạng lớn và IoT, đồng thời cung cấp khả năng tự động và linh hoạt. Tuy nhiên, SLAAC thường chỉ cung cấp địa chỉ IPv6 và Default Gateway mà không bao gồm thông tin DNS Server.

04

DHCPv6 (Dynamic Host Configuration Protocol for IPv6) có những chế độ hoạt động nào và chúng khác nhau ra sao?

DHCPv6 có hai chế độ hoạt động chính:

- Stateful DHCPv6: Tương tự như DHCPv4, máy chủ DHCPv6 sẽ quản lý việc cấp phát địa chỉ IPv6, thông tin DNS và các tùy chọn cấu hình khác cho các thiết bị. Máy chủ lưu trữ trạng thái của các địa chỉ đã được cấp phát để tránh trùng lặp.
- Stateless DHCPv6: Trong chế độ này, các thiết bị vẫn sử dụng SLAAC để tự động cấu hình địa chỉ IPv6 và Default Gateway. Tuy nhiên, chúng sẽ sử dụng DHCPv6 server chỉ để nhận các thông tin cấu hình khác như địa chỉ DNS server và các tùy chọn bổ sung.

Ngoài ra, router còn có thể điều khiển cách cấu hình địa chỉ thông qua các flag trong bản tin RA:

- M Flag (Managed Address Configuration flag): Nếu được đặt là 1, các thiết bị phải sử dụng Stateful DHCPv6 để lấy địa chỉ IPv6 và các thông tin khác.
- O Flag (Other Configuration flag): Nếu được đặt là 1 và M Flag là 0, các thiết bị sẽ sử dụng SLAAC cho địa chỉ IPv6 và Stateless DHCPv6 để lấy các thông tin khác.
- Nếu cả M Flag và O Flag đều là 0: các thiết bị chỉ sử dụng SLAAC và không dùng DHCPv6.

05

Kỹ thuật EUI-64 được sử dụng như thế nào để tạo Interface-ID trong địa chỉ IPv6?

EUI-64 (Extended Unique Identifier) là một phương pháp tạo Interface-ID 64 bit từ địa chỉ MAC 48 bit của thiết bị. Quá trình này bao gồm các bước sau:

1. Tách địa chỉ MAC: Địa chỉ MAC 48 bit được chia thành hai phần 24 bit: Organizationally Unique Identifier (OUI) và Device ID.
2. Chèn FFFE: Chuỗi 16 bit có giá trị hexadecimal FFFE được chèn vào giữa phần OUI và Device ID.
3. Đảo bit U/L: Bit thứ 7 (Universal/Local bit) trong phần OUI sẽ bị đảo ngược (0 thành 1 hoặc 1 thành 0). Kết quả là một Interface-ID 64 bit duy nhất, có thể kết hợp với tiền tố mạng /64 nhận được từ router thông qua SLAAC để tạo thành địa chỉ IPv6 Unicast.

06

Tại sao RFC 4941 đề xuất sử dụng Interface-ID ngẫu nhiên và địa chỉ tạm thời trong IPv6?

RFC 4941 đề xuất sử dụng Interface-ID ngẫu nhiên và địa chỉ tạm thời nhằm tăng cường bảo mật và quyền riêng tư cho người dùng IPv6. Việc tạo Interface-ID từ địa chỉ MAC (thông qua EUI-64) có thể làm lộ thông tin về người dùng và có thể bị theo dõi khi di chuyển giữa các mạng khác nhau. Sử dụng Interface-ID ngẫu nhiên giúp che giấu thông tin này, giảm nguy cơ bị theo dõi và tấn công. Địa chỉ tạm thời là các địa chỉ IPv6 có thời gian tồn tại ngắn hơn địa chỉ chính và được sử dụng cho các kết nối ra bên ngoài Internet. Khi hết thời gian, địa chỉ tạm thời sẽ bị thay thế bằng một địa chỉ ngẫu nhiên mới, giúp tăng cường tính ẩn danh và giảm khả năng bị theo dõi theo thời gian.

Quá trình DAD (Duplicate Address Detection) hoạt động như thế nào trong IPv6?

07

DAD (Duplicate Address Detection) là một cơ chế được sử dụng trong IPv6 để đảm bảo rằng một địa chỉ Unicast (Link Local, Unique Local hoặc Global Unicast) là duy nhất trên một phân đoạn mạng trước khi nó được sử dụng. Quá trình DAD diễn ra như sau:

1. Địa chỉ dự kiến: Khi một thiết bị được gán hoặc tự động cấu hình một địa chỉ IPv6, địa chỉ này sẽ ở trạng thái "dự kiến" (Tentative).
2. Gửi NS: Thiết bị gửi một bản tin Neighbor Solicitation (NS) với địa chỉ nguồn là địa chỉ không xác định (::) và địa chỉ đích là địa chỉ Solicited-Node Multicast tương ứng với địa chỉ IPv6 đang được kiểm tra. Nội dung bản tin NS chứa địa chỉ IPv6 cần kiểm trùng.
3. Kiểm tra phản hồi: Nếu không có thiết bị nào trên mạng đang sử dụng địa chỉ này, thiết bị gửi sẽ không nhận được bất kỳ bản tin Neighbor Advertisement (NA) nào trong một khoảng thời gian nhất định. Lúc này, địa chỉ dự kiến sẽ trở thành địa chỉ hợp lệ và được sử dụng.
4. Phát hiện trùng lặp: Nếu thiết bị gửi nhận được một bản tin NA phản hồi, điều đó có nghĩa là địa chỉ đang được kiểm tra đã được sử dụng bởi một thiết bị khác trên mạng. Trong trường hợp này, thiết bị gửi sẽ không sử dụng địa chỉ đó và có thể thông báo lỗi hoặc cố gắng sử dụng một địa chỉ khác.

Kỹ thuật dò tìm MTU đường truyền (Path MTU Discovery) hoạt động như thế nào trong IPv6 và bản tin ICMPv6 nào liên quan đến quá trình này?

08

Kỹ thuật dò tìm MTU đường truyền (Path MTU Discovery - PMTUD) trong IPv6 cho phép một thiết bị nguồn xác định kích thước gói tin lớn nhất (MTU) có thể được truyền đi trên đường dẫn đến một đích mà không bị phân mảnh. Quá trình này hoạt động như sau:

1. Gửi gói ban đầu: Thiết bị nguồn bắt đầu gửi các gói tin với kích thước bằng MTU của giao diện gửi đi.
2. Bản tin Packet Too Big: Nếu một router trên đường dẫn nhận thấy gói tin quá lớn so với MTU của giao diện tiếp theo, nó sẽ hủy gói tin và gửi một bản tin ICMPv6 Packet Too Big (PTB) trở lại thiết bị nguồn. Bản tin PTB này chứa giá trị MTU mà router hỗ trợ cho chặng tiếp theo.
3. Điều chỉnh kích thước: Thiết bị nguồn nhận được bản tin PTB sẽ giảm kích thước gói tin xuống giá trị MTU được chỉ định và thử gửi lại. Quá trình này lặp lại cho đến khi gói tin đến đích mà không nhận phải bản tin PTB nào.
4. Lưu trữ MTU đường truyền: Thiết bị nguồn sẽ lưu trữ giá trị MTU đường truyền đã tìm được cho cặp địa chỉ nguồn và đích trong bộ nhớ Cache để sử dụng cho các kết nối sau này.

PHẦN 1 – LÝ THUYẾT

CHƯƠNG 5

CÁC KỸ THUẬT CHUYỂN ĐỔI TỪ IPv4 SANG IPv6

CHƯƠNG 5

CÁC KỸ THUẬT CHUYỂN ĐỔI TỪ IPv4 SANG IPv6

Việc chuyển đổi từ IPv4 sang IPv6 là một thách thức lớn do có sự khác biệt về cấu trúc và cách thức hoạt động giữa hai giao thức. Bên cạnh đó, mỗi hệ thống mạng của các doanh nghiệp, tổ chức lại có đặc thù riêng về quy mô, công nghệ và loại hình dịch vụ nên không thể áp dụng một giải pháp chuyển đổi chung cho tất cả hệ thống. Để giải quyết vấn đề này, nhiều kỹ thuật chuyển đổi đã được đề xuất với những ưu và nhược điểm riêng. Việc lựa chọn đúng giải pháp sẽ đảm bảo quá trình chuyển đổi diễn ra suôn sẻ, hiệu quả và tiết kiệm.

Chương này bắt đầu với những thách thức và yêu cầu mà các tổ chức phải đối mặt do sự khác biệt giữa hai giao thức. Sau đó, nó giới thiệu và phân tích chi tiết ba kỹ thuật chuyển đổi chính: Dual Stack (hoạt động đồng thời cả hai giao thức), Tunneling (đóng gói IPv6 trong IPv4) và Translation (chuyển đổi địa chỉ giữa hai giao thức), làm rõ ưu nhược điểm của từng phương pháp. Đặc biệt, chương này còn đề cập đến các giải pháp triển khai IPv6 trong mạng MPLS, như 6PE và 6VPE. Cuối cùng là lộ trình chuyển đổi IPv6 tại Việt Nam do VNNIC đề xuất, bao gồm các giai đoạn chuẩn bị, thử nghiệm và chuyển đổi chính thức. Mục đích của chương là cung cấp kiến thức toàn diện về các kỹ thuật và kế hoạch chuyển đổi, giúp các tổ chức có thể lựa chọn và thực hiện quá trình này một cách hiệu quả.

Chương này giúp bạn nắm được những nội dung sau:

Những thách thức và yêu cầu cơ bản trong quá trình chuyển đổi từ IPv4 sang IPv6. Bạn sẽ hiểu rằng đây là một kế hoạch dài hạn đòi hỏi sự chuẩn bị kỹ lưỡng về nguồn lực, lập kế hoạch chi tiết và lựa chọn kỹ thuật phù hợp.

Kỹ thuật Dual Stack: là một trong những kỹ thuật chuyển đổi phổ biến nhất, cho phép các thiết bị hoạt động đồng thời trên cả hai giao thức IPv4 và IPv6. Bạn sẽ nắm được **ưu điểm** của Dual Stack cũng như những **thách thức** của kỹ thuật này.

Kỹ thuật Tunneling: cho phép truyền gói tin IPv6 qua mạng IPv4 bằng cách đóng gói chúng trong các gói IPv4 . Bạn sẽ hiểu tại sao kỹ thuật này thường được sử dụng khi không thể triển khai Dual Stack nhưng cũng có những **hạn chế**.

Kỹ thuật Translation: cho phép các thiết bị thuần IPv6 và thuần IPv4 giao tiếp trực tiếp thông qua việc "biên dịch" địa chỉ cùng những **ưu và hạn chế**. Tuy vậy, Translation vẫn là một giải pháp quan trọng trong giai đoạn chuyển đổi, đặc biệt hướng tới IPv6 Only.

Chuyển đổi IPv6 cho mạng MPLS: một công nghệ quan trọng trong các hệ thống mạng lớn của nhà mạng. Chương này giới thiệu hai kỹ thuật chuyển đổi IPv6 riêng cho mạng MPLS là **6PE (IPv6 Provider Edge) và 6VPE (IPv6 VPN Provider Edge).**

Lộ trình chuyển đổi IPv6 tại Việt Nam, bao gồm các giai đoạn chuẩn bị, kết nối và thử nghiệm và chuyển đổi chính thức. Bạn sẽ hiểu về vai trò của VNNIC trong việc xây dựng và thúc đẩy lộ trình này với 3 giai đoạn và 10 bước thực hiện chi tiết.

Tóm lại, chương 5 cung cấp một cái nhìn toàn diện về các kỹ thuật và lộ trình chuyển đổi từ IPv4 sang IPv6, giúp các tổ chức và doanh nghiệp có thể lựa chọn phương pháp phù hợp để triển khai IPv6 một cách hiệu quả và bền vững.

5.1. NHỮNG THÁCH THỨC VÀ YÊU CẦU

Việc chuyển đổi từ IPv4 sang IPv6 đặt ra nhiều thách thức đáng kể do sự khác biệt cơ bản giữa hai giao thức. Các tổ chức buộc phải lựa chọn kỹ lưỡng giải pháp chuyển đổi như Dual Stack, Tunneling hoặc Translation. Việc lựa chọn không chỉ ảnh hưởng đến quá trình chuyển đổi mà còn tác động đến công tác quản lý và vận hành hệ thống mạng cả trong và sau khi chuyển đổi.

Một vấn đề khác là việc hỗ trợ IPv6 của các ứng dụng và phần mềm. Nhiều ứng dụng cũ chỉ hỗ trợ IPv4, đòi hỏi phải nâng cấp hoặc viết lại để tương thích với IPv6. Quá trình này đòi hỏi chi phí lớn và thời gian thực hiện kéo dài. Đặc biệt, các ứng dụng hoặc chính sách phụ thuộc vào địa chỉ IP, như hệ thống tường lửa hoặc cơ chế xác thực, phải được cấu hình lại cẩn thận để tránh gián đoạn hoạt động và xả ra các vấn đề về bảo mật.

Hạ tầng mạng và các thiết bị mạng hiện tại cũng là một thách thức không nhỏ. Nhiều thiết bị không hỗ trợ hoặc chỉ hỗ trợ IPv6 một phần. Điều này đòi hỏi các tổ chức, doanh nghiệp phải đầu tư nâng cấp hoặc thay thế thiết bị, làm gia tăng đáng kể chi phí. Hơn nữa, quá trình thay đổi này còn tiềm ẩn nguy cơ gián đoạn dịch vụ, ảnh hưởng đến người dùng trong thời gian triển khai.

Việc định tuyến và quản lý mạng trong môi trường IPv6 cũng đặt ra những yêu cầu mới. IPv6 kéo theo sự nâng cấp và bổ sung nhiều giao thức mới như: OSPFv3, VRRPv6, DHCPv6, NDP và NPTv6 ... Việc này đòi hỏi các kỹ sư mạng phải làm quen và nắm bắt chúng. Bên cạnh đó, quy mô địa chỉ khổng lồ của IPv6 (2^128 địa chỉ) yêu cầu những phương pháp phân bổ và quản lý địa chỉ hoàn toàn khác biệt so với IPv4.

Bảo mật là một lĩnh vực không thể bỏ qua trong quá trình chuyển đổi. Mặc dù IPv6 tích hợp sẵn IPSec để tăng cường bảo mật, điều này không có nghĩa là hệ thống sẽ an toàn hơn. Trong môi trường hỗn hợp Dual Stack, nơi IPv4 và IPv6 cùng hoạt động, người quản trị cần đảm bảo khai báo bảo mật nhằm giảm thiểu rủi ro, duy trì tính ổn định của hệ thống mạng.

Bên cạnh đó, việc đào tạo và phát triển kỹ năng cho đội ngũ quản trị mạng là một yêu cầu rất quan trọng. Đội ngũ này cần được trang bị kiến thức từ cơ bản đến chuyên sâu về IPv6, bao gồm các kỹ thuật cấu hình, khai báo bảo mật, định tuyến và xử lý sự cố. Đặc biệt, kỹ năng vận hành trong các môi trường như Dual Stack hoặc IPv6 Only là yếu tố đảm bảo hệ thống hoạt động ổn định, hiệu quả trong suốt quá trình chuyển đổi và giai đoạn vận hành sau đó.

Như vậy, chuyển đổi từ IPv4 sang IPv6 không chỉ là một quyết định mang tính kỹ thuật mà còn là một kế hoạch dài hạn đòi hỏi sự chuẩn bị kỹ lưỡng. Để đảm bảo thành công thì các tổ chức, doanh nghiệp cần tập trung vào việc chuẩn bị nguồn lực, lập kế hoạch chi tiết và lựa chọn kỹ thuật phù hợp với đặc thù hệ thống mạng của mình.

5.2. KỸ THUẬT DUAL STACK

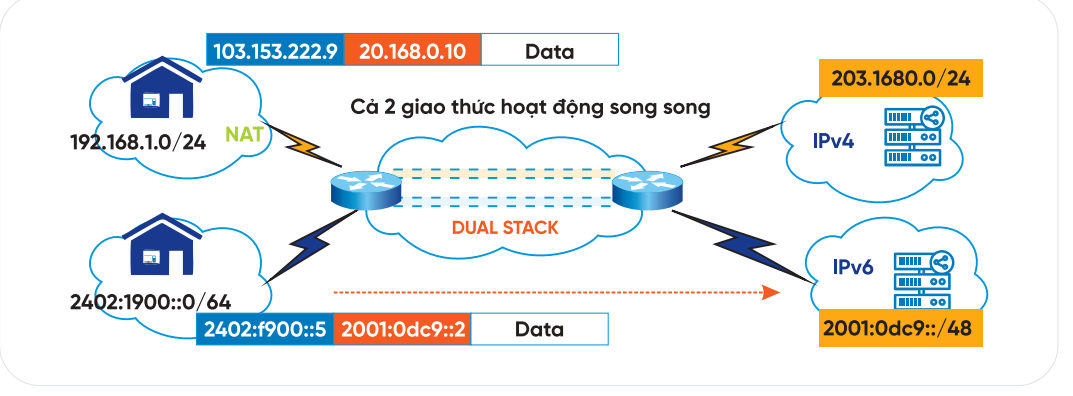
Đây là kỹ thuật được áp dụng phổ biến nhất trong thực tế dù vẫn tồn một số hạn chế. Kỹ thuật này cho phép các thiết bị mạng hoạt động đồng thời trên cả hai giao thức IPv4 và IPv6, thiết bị tự quyết định sử dụng giao thức nào dựa trên khả năng kết nối là IPv4 hay IPv6 và thông tin từ các bản ghi DNS.

Ưu điểm nổi bật của Dual Stack là kỹ thuật này không yêu cầu thay đổi hệ thống mạng hiện tại, không làm ảnh hưởng dịch vụ, có khả năng triển khai theo từng giai đoạn và đội ngũ tham gia có thể tiếp cận dần dần. Các tổ chức có thể bắt đầu chuyển đổi từ các phân vùng mạng nhỏ hoặc không quan trọng trước, sau đó dần mở rộng ra toàn bộ hệ thống, hoàn thành chuyển đổi hạ tầng rồi đến dịch vụ. Điều này giúp giảm thiểu rủi ro, tránh áp lực phải chuyển đổi hoàn toàn hệ thống ngay lập tức.

Tuy nhiên, Dual Stack cũng đi kèm với một số thách thức. Việc sử dụng đồng thời IPv4 và IPv6 làm tăng độ phức tạp khi khai báo, khó khăn trong vận hành khai thác và đặc biệt ảnh hưởng đến hiệu suất thiết bị khi phải duy trì, xử lý cả hai giao thức. Do vẫn duy trì giao thức IPv4 nên kỹ thuật này vẫn phụ thuộc vào tài nguyên địa chỉ IPv4 hiện đang rất khan hiếm nên có thể ảnh hưởng đến hệ thống và dịch vụ một thời điểm nào đó.

Về mặt bảo mật thì khả năng các hệ thống Dual Stack bị tấn công cả ở môi trường IPv4 và IPv6 nên đây cũng là thách thức rất lớn trong việc thiết lập và duy trì các chính sách bảo mật. Các chính sách bảo mật (Policy) cần được khai báo cho cả hai giao thức và các chính sách cho IPv6 gần như tương đương với chính sách hiện có của IPv4, chỉ khác địa chỉ đích. Nói cách khác, các Access Control List (ACL) kiểm soát truy cập trên các thiết bị sẽ được nhân đôi. Việc thiếu sót khai báo bảo mật cho IPv6 sẽ gây ra lỗ hổng rất lớn cho hệ thống. Các chính sách bảo mật cho IPv6 cần phải được khai báo trước khi khai báo địa chỉ IPv6 trên các thiết bị. Và một điều nữa, nếu đã sử dụng cơ chế chuyển đổi Dual Stack thì không nên áp dụng thêm các cơ chế khác vì khó kiểm soát những vấn đề phát sinh và làm phức tạp thêm quá trình chuyển đổi.

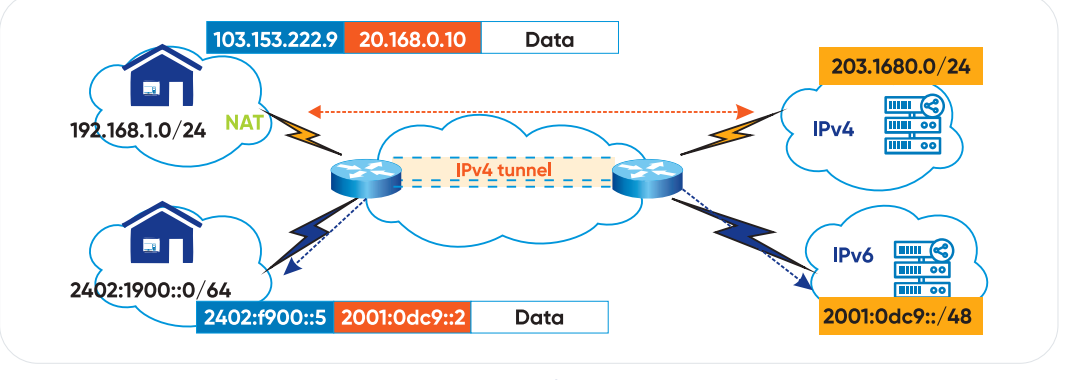
Dual Stack là giải pháp được nhiều tổ chức lựa chọn triển khai trong thực tế vì sự an toàn và ổn định mà nó mang lại trong quá trình chuyển đổi. Mặt khác kỹ thuật này cũng được xem là bước đệm lý tưởng để chuyển hệ thống sang hoạt động với chế độ IPv6 Only.



Hình 84. Hoạt động của cơ chế Dual Stack

5.3. KỸ THUẬT TUNNELING

Tunneling là kỹ thuật đóng gói (Encapsulation) cho phép các gói tin IPv6 được truyền qua mạng IPv4 bằng cách gói chúng trong các gói IPv4 và có khá nhiều kỹ thuật chuyển đổi thuộc nhóm này. Điều này đặc biệt hữu ích trong các mạng mà hạ tầng IPv4 vẫn chiếm ưu thế. Có một câu nói trong quá trình chuyển đổi IPv6 đó là **"Dual stack where you can; tunnel where you must"**. Kỹ thuật đường hầm Tunneling không được đánh giá cao so với Dual Stack vì vẫn sử dụng hạ tầng của mạng IPv4, làm tăng độ trễ và tiêu tốn thêm tài nguyên xử lý do phải đóng, mở gói tin, đặc biệt trong các mạng có lưu lượng cao.



Hình 85. Hoạt động của cơ chế Tunnel

Ngoài hạn chế này Tunneling cũng tồn tại những vấn đề liên quan đến bảo mật. Một số kỹ thuật như 6to4, 6RD, ISATAP, Teredo, Tunnel Broker ... đóng gói dữ liệu IPv6 trong các bản tin IPv4 dẫn đến bản tin IPv6 sẽ không được kiểm soát (Bypass). Các thiết bị bảo mật không thể kiểm tra đồng thời cả hai giao thức. Do đó hệ thống IPv6 bên trong có thể bị tấn công thông qua môi trường IPv4. RFC 3964 đã mô tả rất chi tiết những cách tấn công thông qua 6to4 Tunnel, còn kỹ thuật 6RD kế thừa những đặc điểm như của 6to4 nên vẫn có chung vấn đề.

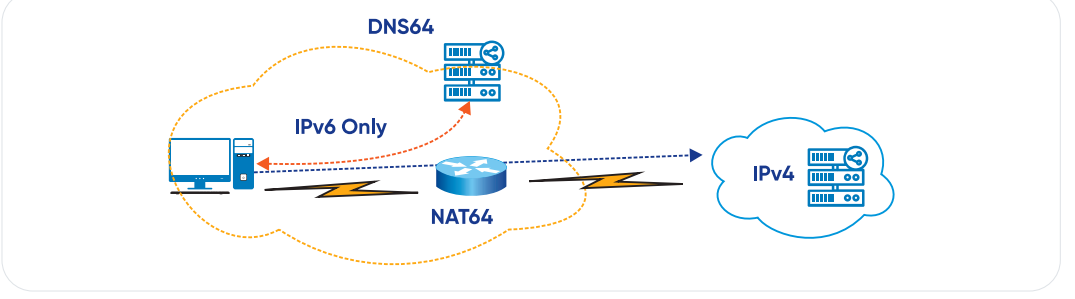
KỸ THUẬT TUNNELING	MÔ TẢ	ỨNG DỤNG CHÍNH
6in4	Đóng gói gói tin IPv6 trong gói tin IPv4 để truyền qua mạng IPv4, không yêu cầu cấu hình phức tạp.	Kết nối mạng IPv6 qua hạ tầng IPv4.
6to4	Tự động tạo đường hầm dựa trên địa chỉ IPv4 công cộng, sử dụng tiền tố 2002::/16.	Mạng không có kết nối IPv6 trực tiếp.
Teredo	Sử dụng UDP để đóng gói IPv6, vượt qua NAT IPv4, hỗ trợ thiết bị sau NAT.	Người dùng cuối sau NAT.
ISATAP	Tự động tạo đường hầm trong mạng nội bộ IPv4, gán địa chỉ IPv6 cho các máy chủ.	Mạng doanh nghiệp nội bộ.
GRE	Gói tin IPv6 được đóng gói trong IPv4 bằng giao thức Generic Routing Encapsulation.	Hỗ trợ đa giao thức, cấu hình trên router.
6rd	Cải tiến của 6to4, sử dụng địa chỉ IPv4 của khách hàng để tạo địa chỉ IPv6 nhanh chóng.	Triển khai IPv6 tại nhà cung cấp dịch vụ.
DS-Lite	Kết hợp Tunneling với NAT44, truyền IPv6 qua IPv4 với hỗ trợ từ nhà cung cấp.	Mạng hỗ trợ chuyển đổi Dual Stack.
MAP-T	Sử dụng Tunneling với ánh xạ địa chỉ và cổng để chuyển đổi giữa IPv4 và IPv6.	Nhà cung cấp dịch vụ hỗ trợ IPv6.
LISP	Tách biệt định danh và định vị, hỗ trợ truyền IPv6 qua IPv4 bằng đường hầm.	Giải pháp định tuyến linh hoạt.
IP-in-IP	Đóng gói gói tin IPv6 trong IPv4 hoặc ngược lại bằng cơ chế cơ bản.	Ứng dụng hạn chế do thiếu bảo mật.

Bảng 8. Tóm tắt một số kỹ thuật Tunnel

Vì thế nên hạn chế sử dụng cơ chế Tunneling. Nếu cần sử dụng thì chỉ áp dụng ở phạm vi cần thiết và có chính sách bảo mật kỹ lưỡng cho các thiết bị sử dụng IPv6 bên trong. Trong thực tế, kỹ thuật Tunneling được áp dụng nhiều nhất cho mạng chuyển mạch nhãn MPLS (Multiprotocol Label Switching), công nghệ này được áp dụng trong các nhà mạng hay hệ thống mạng MAN tại một số địa phương, tổ chức.

5.4. KỸ THUẬT TRANSLATION

Translation (chuyển đổi giao thức) là kỹ thuật cho phép các thiết bị thuần IPv6 (IPv6 Only) và thuần IPv4 (IPv4 Only) giao tiếp trực tiếp với nhau. Cách thức hoạt động của kỹ thuật này là "biên dịch" địa chỉ của các bản tin từ IPv6 sang IPv4 và ngược lại. Có hai kỹ thuật chính cho giải pháp này là NAT64 và NAT46. NAT64 cho phép các thiết bị IPv6 Only kết nối với các dịch vụ hoặc ứng dụng chỉ hỗ trợ IPv4 Only. Ngược lại, NAT46 hỗ trợ các hệ thống IPv4 Only truy cập các dịch vụ hoạt động trên IPv6 Only. Hai kỹ thuật này thường được sử dụng trong thực tế, đặc biệt ở các mạng cần triển khai IPv6 Only.



Hình 86. Kỹ thuật NAT cho mạng IPv6 Only

Ưu điểm lớn nhất của Translation là bảo đảm khả năng tương thích ngược, cho phép các hệ thống IPv4 và IPv6 giao tiếp mà không cần nâng cấp toàn bộ hạ tầng mạng. Điều này giúp các tổ chức, doanh nghiệp tiết kiệm chi phí và thời gian trong giai đoạn chuyển đổi. Translation cũng cho phép triển khai từng bước, có thể triển khai thử nghiệm IPv6 trên một phần hệ thống trước khi tiến hành trên diện rộng. Giải pháp này đóng vai trò như một bước đệm để khai thác những ưu điểm của IPv6 mà không làm gián đoạn các dịch vụ IPv4 hiện có.

Tuy nhiên, Translation cũng có những hạn chế đáng kể. Việc chuyển đổi địa chỉ của gói tin từ giao thức này sang giao thức kia sẽ làm tăng độ trễ và giảm hiệu suất mạng, đặc biệt trong các hệ thống có lưu lượng lớn và yêu cầu tốc độ cao. Ngoài ra, Translation phá vỡ tính kết nối toàn tuyến (End-to-End) vốn là một ưu điểm của IPv6, gây khó khăn trong việc triển khai các giải pháp bảo mật như IPSec, DNSSec.

Dù có những hạn chế, Translation vẫn là một giải pháp quan trọng trong giai đoạn chuyển đổi, nhất là khi các tổ chức chưa sẵn sàng áp dụng IPv6 hoàn toàn, đặc biệt là trong kế hoạch tiến tới triển khai IPv6 Only.

Ba giải pháp chuyển đổi từ IPv4 sang IPv6 trình bày ở trên đều có ưu, nhược điểm riêng, đồng thời cho phép lựa chọn phù hợp với từng tình huống triển khai cụ thể. Việc lựa chọn giải pháp nào cần cân nhắc kỹ lưỡng các yếu tố như chi phí, hiệu suất, tính ổn định và mục tiêu dài hạn, nhằm đảm bảo quá trình chuyển đổi sang IPv6 diễn ra hiệu quả và bền vững.

5.5. CHUYỂN ĐỔI IPv6 CHO MẠNG MPLS

Công nghệ chuyển mạch nhãn MPLS (Multiprotocol Label Switching) là một công nghệ tiên tiến được sử dụng rất phổ biến trong các hệ thống mạng lớn, cung cấp đa dịch vụ như của các nhà mạng (ISP) hay trạm trung chuyển Internet (IXP). Các hệ thống mạng MPLS về quy mô có thể ở phạm vi của một hoặc vài quốc gia và có cung cấp rất nhiều dịch vụ quan trọng như 4G, 5G, FTTH, IP Leased Line, IPTV ... Vì thế việc chuyển đổi IPv6 cho các mạng MPLS rất phức tạp và có thể ảnh hưởng rất nhiều dịch vụ và gây tác động lớn.

Mặt khác, có nhiều giao thức được triển khai trong mạng MPLS như IGP, LDP, RSVP, nếu chuyển đổi sang IPv6 thì cần phải nâng cấp, thay thế các giao thức này để hỗ trợ IPv6. Việc này thực sự rất mất thời gian và phức tạp. Nhiều hãng sản xuất thiết bị không mặn mà với việc này. Ngoài ra RFC 7439 (Gap Analysis for Operating IPv6-Only MPLS Networks) cũng đã phân tích rất rõ những vấn đề gặp phải khi chuyển mạng MPLS sang hoạt động với chế độ IPv6 Only.

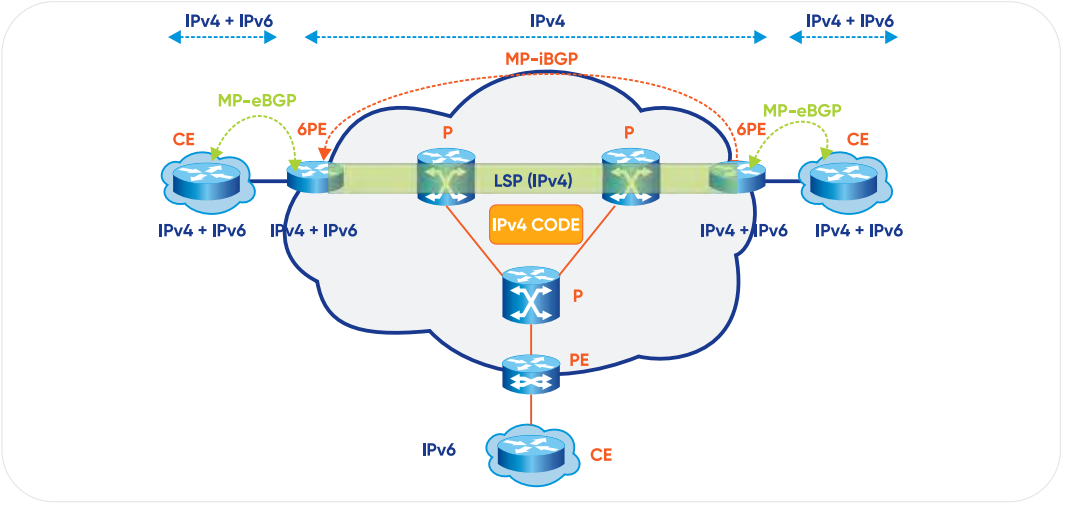
Một lợi thế của mạng MPLS là hiện đã có những LSP (Label Switched Path) giữa các PE Router (Provider Edge) được thiết lập trên nền IPv4. Đây là những Tunnel được tạo tự động bằng LDP (Label Distribution Protocol) hoặc bằng RSVP (Resource Reservation Protocol) nên cần một giải pháp để tận dụng những Tunnel này để truyền tải dữ liệu IPv6 theo kỹ thuật Tunneling được giới thiệu ở phần trước.

Chính vì thế đã có một giải pháp chuyển đổi IPv6 riêng dành cho mạng MPLS bao gồm hai kỹ thuật là 6PE (IPv6 Provider Edge) và 6VPE (IPv6 VPN Provider Edge). Sau đây là thông tin chi tiết của 6PE và 6VPE:

5.5.1. 6PE (IPv6 Provider Edge)

6PE (IPv6 Provider Edge) là một kỹ thuật cho phép các gói tin IPv6 được vận chuyển qua mạng MPLS thông qua các LSP chạy IPv4 Only mà không cần nâng cấp hoặc chuyển đổi mạng lõi sang IPv6. Cơ chế hoạt động của 6PE dựa trên việc các router biên (PE Router) hoạt động với cả IPv4 và IPv6 (chế độ Dual Stack). Tại router PE nguồn, các gói tin IPv6 được "đóng nhãn MPLS" rồi được vận chuyển qua thông qua các LSP được thiết lập trước thông qua IPv4. Các router trung gian sẽ chỉ xử lý nhãn MPLS mà không cần biết thông bên trong là IPv4 hay IPv6. Khi đến Router PE đích, các gói tin sẽ được "gỡ nhãn" để tiếp tục xử lý dưới dạng IPv6.

6PE có đặc điểm nổi bật là tận dụng mạng MPLS IPv4 hiện có, giúp giảm thiểu nhu cầu nâng cấp mạng lõi và cho phép triển khai IPv6 dễ dàng và nhanh chóng. Đây là một giải pháp phù hợp cho các nhà mạng muốn triển khai IPv6 từng bước mà vẫn giữ được hạ tầng MPLS hiện tại. Về ưu điểm, 6PE giúp giảm chi phí và thời gian để nâng cấp mạng lõi, đồng thời đảm bảo hiệu suất cao nhờ hoạt động đóng gỡ nhãn MPLS và dữ liệu được truyền đi qua các LSP sẵn có. Ngoài ra, nó tương thích tốt với các giao thức định tuyến IPv6 như BGP, giúp mạng hoạt động ổn định trong quá trình chuyển đổi.



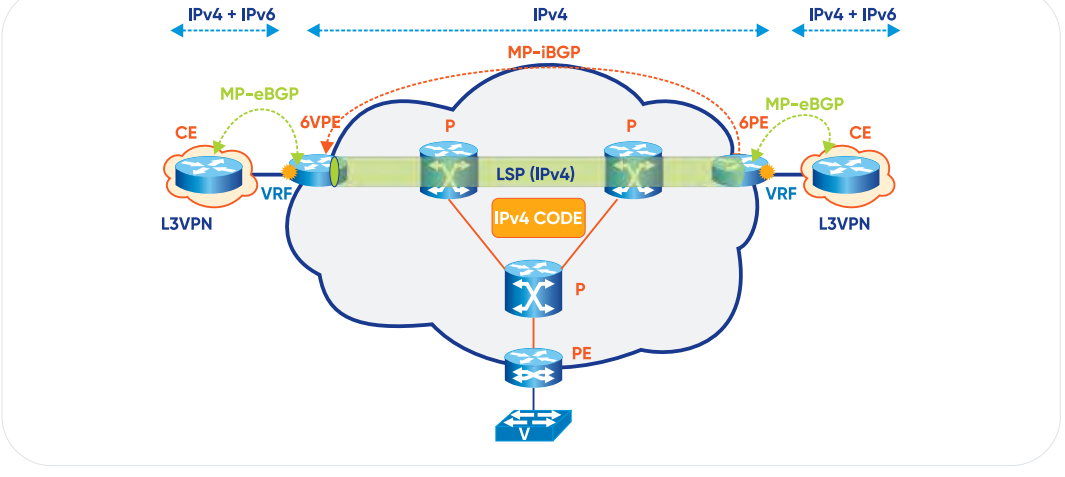
Hình 87. Hoạt động của cơ chế 6PE

Tuy nhiên, 6PE cũng có một số hạn chế cần lưu ý. Việc triển khai 6PE phụ thuộc vào khả năng hỗ trợ IPv6 của các router biên, đồng thời không hỗ trợ các dịch vụ VPN phức tạp. Vì vậy, các tổ chức cần cân nhắc kỹ lưỡng về hạ tầng mạng và mục tiêu dịch vụ khi lựa chọn kỹ thuật này.

5.5.2. 6VPE (IPv6 VPN Provider Edge)

6VPE (IPv6 VPN Provider Edge) là một cơ chế mở rộng từ 6PE, cho phép triển khai dịch vụ VPN IPv6 trên mạng MPLS hiện có. Kỹ thuật này được sử dụng phổ biến hơn so với 6PE vì trong thực tế các dịch vụ trên mạng MPLS phần lớn sử dụng VPN. Trong mô hình này, các PE Routers xử lý đồng thời cả lưu lượng IPv4 VPN và IPv6 VPN bằng cách sử dụng các bảng định tuyến riêng biệt cho từng khách hàng, được gọi là VRF (Virtual Routing and Forwarding). Lưu lượng IPv6 VPN được "đóng gói" bằng nhãn MPLS riêng để vận chuyển qua mạng giống như cơ chế của 6PE, đảm bảo tính tách biệt và bảo mật giữa các khách hàng.

Đồng thời, giải pháp này mang lại tính linh hoạt cao khi cho phép hỗ trợ song song cả IPv4 VPN và IPv6 VPN trên cùng một hạ tầng mạng lõi đang sử dụng IPv4 Only. Những ưu điểm chính của 6VPE bao gồm việc tận dụng mạng MPLS hiện tại, tích hợp dễ dàng với các dịch vụ VPN của khách hàng và đảm bảo tính bảo mật cao nhờ khả năng tách biệt lưu lượng giữa các khách hàng.



Hình 88. Hoạt động của cơ chế 6VPE

Việc triển khai 6VPE sẽ cấu hình phức tạp hơn so với 6PE, tuy nhiên đây vẫn là giải pháp tối ưu cho các nhà cung cấp dịch vụ cần triển khai IPv6 VPN trên hạ tầng MPLS mà không làm gián đoạn hoạt động của mạng lõi.

5.6. XÂY DỰNG KẾ HOẠCH CHUYỂN ĐỔI IPv6

Kế hoạch chuyển đổi từ IPv4 sang IPv6 đòi hỏi sự chuẩn bị kỹ lưỡng và một lộ trình chi tiết, đảm bảo tính liên tục của dịch vụ và phù hợp với đặc thù của từng lĩnh vực như doanh nghiệp, mạng cố định và mạng di động.

Lộ trình này cần được xây dựng theo từng giai đoạn rõ ràng, bao gồm:

- Khảo sát, đánh giá hiện trạng hệ thống và lập kế hoạch chi tiết.
- Thử nghiệm triển khai song song IPv4/IPv6 (Dual Stack) hoặc sử dụng kỹ thuật Tunneling cho quy mô nhỏ để đảm bảo hoạt động ổn định.
- Mở rộng ứng dụng IPv6 trên toàn hệ thống.
- Chuyển đổi hoàn toàn sang IPv6 khi điều kiện cho phép, sử dụng kỹ thuật Translation.

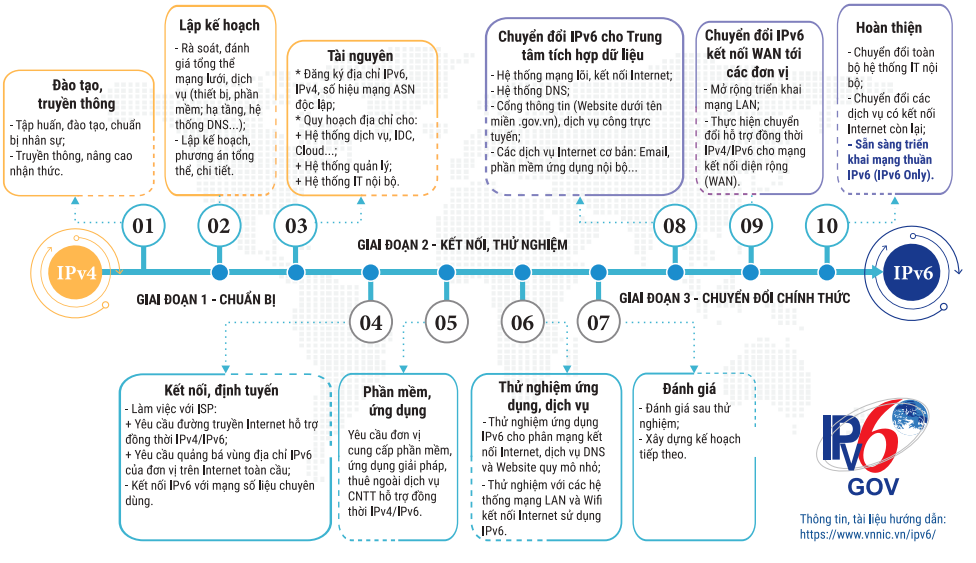
Bên cạnh các yếu tố kỹ thuật, việc đào tạo nhân sự, nâng cao nhận thức thông qua truyền thông và phối hợp chặt chẽ giữa các bên liên quan cũng là những yếu tố quan trọng. Một lộ trình được thiết kế bài bản không chỉ giúp tổ chức sẵn sàng cho IPv6 mà còn tạo nền tảng vững chắc cho quá trình chuyển đổi số trong tương lai.

Trung tâm Internet Việt Nam (VNNIC) với vai trò thúc đẩy chuyển đổi IPv6 trong nước trong nhiều năm qua, đã xây dựng Tài liệu hướng dẫn chuyển đổi IPv6 dành cho các cơ quan nhà nước và có thể nhân rộng áp dụng cho các đơn vị khác. Kế hoạch bao gồm 3 giai đoạn với 10 bước thực hiện chi tiết, nhằm thúc đẩy việc ứng dụng IPv6 tại Việt Nam một cách có hệ thống và hiệu quả. Dưới đây là chi tiết các giai đoạn và bước thực hiện:

5.6.1. Giai đoạn 1: Chuẩn bị

Mục tiêu: Xây dựng nền tảng vững chắc, đảm bảo nhận thức, nhân lực và tài nguyên kỹ thuật sẵn sàng cho quá trình chuyển đổi.

- **Bước 1:** Đào tạo nhân sự, tuyên truyền nâng cao nhận thức về IPv6.
- **Bước 2:** Rà soát hạ tầng, đánh giá khả năng hỗ trợ IPv6 của mạng lưới, thiết bị, phần mềm.
- **Bước 3:** Đăng ký địa chỉ IPv6 và tái quy hoạch tài nguyên mạng theo tiêu chuẩn mới.



Hình 89. Kế hoạch 03 Giai đoạn - 10 bước chuyển đổi IPv6

5.6.2. Giai đoạn 2: Kết nối và thử nghiệm

Mục tiêu: Đảm bảo khả năng kết nối IPv6 trên toàn hệ thống, thử nghiệm thực tế và từng bước triển khai các dịch vụ quan trọng.

- **Bước 4:** Kết nối IPv6 với mạng Internet, làm việc với ISP để đảm bảo đường truyền hỗ trợ song song IPv4/IPv6.
- **Bước 5:** Kiểm tra và chuyển đổi phần mềm, ứng dụng nội bộ sang IPv6.
- **Bước 6:** Thử nghiệm dịch vụ trên nền IPv6, bao gồm Website, Email, hệ thống DNS và mạng LAN/Wi-Fi nội bộ.
- **Bước 7:** Đánh giá kết quả thử nghiệm, giám sát và điều chỉnh trước khi chuyển đổi chính thức.

5.6.3. Giai đoạn 3: Chuyển đổi chính thức

Mục tiêu: Hoàn thiện quá trình chuyển đổi, đảm bảo hệ thống hoạt động ổn định trên nền IPv6, hướng đến triển khai IPv6 hoàn toàn.

- **Bước 8:** Mở rộng triển khai IPv6 cho hệ thống trung tâm dữ liệu, các dịch vụ công trực tuyến và ứng dụng nội bộ.
- **Bước 9:** Chuyển đổi toàn bộ mạng lưới WAN, liên kết IPv6 giữa các đơn vị, đảm bảo vận hành song song với IPv4 trước khi cắt giảm.
- **Bước 10:** Hoàn tất quá trình chuyển đổi, đánh giá toàn diện và hướng đến việc triển khai "IPv6 Only" trong tương lai.

Kế hoạch chuyển đổi IPv6 không chỉ tập trung vào các bước kỹ thuật mà còn nhấn mạnh vai trò của đào tạo, truyền thông và giám sát, tạo nên một mô hình chuyển đổi toàn diện. Tài liệu mẫu giúp cơ quan, đơn vị xây dựng và triển khai tốt công tác IPv6, góp phần quan trọng cho công tác chuyển đổi IPv6 Việt Nam, đặc biệt trong bối cảnh chiến lược chuyển đổi số quốc gia hướng tới mục tiêu dài hạn như IPv6 Only trong tương lai.

5.7. TỔNG KẾT CHƯƠNG 5

Chương 5 đã trình bày chi tiết về các kỹ thuật chuyển đổi từ IPv4 sang IPv6, một quá trình tất yếu để đáp ứng nhu cầu mở rộng không gian địa chỉ và nâng cao hiệu suất mạng. Nội dung chương đã phân tích những thách thức và yêu cầu đặt ra khi triển khai IPv6, từ đó giới thiệu các giải pháp kỹ thuật phổ biến như Dual Stack, Tunneling và Translation, giúp đảm bảo khả năng tương thích giữa hai giao thức trong giai đoạn chuyển đổi. Bên cạnh đó, chương 5 cũng đề cập đến các kỹ thuật triển khai IPv6 trong mạng MPLS, đặc biệt là các giải pháp 6PE và 6VPE, giúp các nhà cung cấp dịch vụ mạng có thể hỗ trợ IPv6 mà không cần thay đổi toàn bộ hạ tầng hiện có. Ngoài ra, chương này cũng cung cấp cái nhìn tổng quan về cách thức xây dựng và triển khai kế hoạch chuyển đổi IPv6 cho mạng cơ quan, doanh nghiệp, với ba giai đoạn từ chuẩn bị, thử nghiệm cho đến chuyển đổi chính thức. Việc hiểu rõ các kỹ thuật và lộ trình này sẽ giúp các tổ chức, doanh nghiệp và nhà quản lý mạng có kế hoạch triển khai IPv6 một cách hiệu quả, tối ưu hóa tài nguyên mạng và đảm bảo sự phát triển bền vững của hệ thống trong tương lai.

5.8. CÂU HỎI ÔN TẬP CHƯƠNG 5

01

Tại sao cần phải chuyển đổi từ IPv4 sang IPv6?

Việc chuyển đổi từ IPv4 sang IPv6 là cần thiết do không gian địa chỉ IPv4 (khoảng 4,3 tỷ địa chỉ) ngày càng cạn kiệt, không đáp ứng được sự phát triển nhanh chóng của Internet và các thiết bị kết nối. IPv6 cung cấp một không gian địa chỉ khổng lồ (khoảng 340 tỷ tỷ tỷ địa chỉ), giải quyết triệt để vấn đề này và mở ra khả năng kết nối không giới hạn cho tương lai.

02

Những thách thức chính khi chuyển đổi từ IPv4 sang IPv6 là gì?

Quá trình chuyển đổi IPv4 sang IPv6 đối mặt với nhiều thách thức, bao gồm sự khác biệt cơ bản giữa hai giao thức đòi hỏi lựa chọn kỹ lưỡng các giải pháp chuyển đổi (Dual Stack, Tunneling, Translation); sự tương thích của các ứng dụng và phần mềm cũ; yêu cầu nâng cấp hoặc thay thế các thiết bị mạng hiện tại; những phức tạp trong định tuyến và quản lý mạng IPv6 với các giao thức mới; các vấn đề về bảo mật trong môi trường hỗn hợp và nhu cầu đào tạo đội ngũ quản trị mạng.

03

Kỹ thuật Dual Stack là gì và nó hoạt động như thế nào trong quá trình chuyển đổi IPv6?

Dual Stack là một kỹ thuật cho phép các thiết bị mạng hoạt động đồng thời với cả hai giao thức IPv4 và IPv6. Thiết bị sẽ tự động quyết định sử dụng giao thức nào dựa trên khả năng kết nối và thông tin từ DNS. Ưu điểm của Dual Stack là không yêu cầu thay đổi hệ thống mạng hiện tại, có thể triển khai từng giai đoạn, giảm thiểu rủi ro. Tuy nhiên, nó cũng làm tăng độ phức tạp trong cấu hình, vận hành và có thể ảnh hưởng đến hiệu suất thiết bị do phải duy trì cả hai giao thức.

04

Kỹ thuật Tunneling được sử dụng như thế nào để truyền dữ liệu IPv6 qua mạng IPv4?

Kỹ thuật Tunneling cho phép đóng gói các gói tin IPv6 bên trong các gói tin IPv4 để truyền qua mạng IPv4. Có nhiều kỹ thuật Tunneling khác nhau như 6in4, 6to4, Teredo, ISATAP... Kỹ thuật này hữu ích khi cần kết nối các mạng IPv6 qua hạ tầng IPv4 hiện có. Tuy nhiên, Tunneling có thể làm tăng độ trễ, tiêu tốn tài nguyên xử lý và tiềm ẩn các vấn đề bảo mật do các gói tin IPv6 có thể không được kiểm soát đầy đủ.

05

Kỹ thuật Translation (NAT64/NAT46) giúp các mạng IPv4 và IPv6 giao tiếp với nhau ra sao?

Kỹ thuật Translation cho phép các thiết bị thuần IPv6 (IPv6 Only) và thuần IPv4 (IPv4 Only) giao tiếp trực tiếp bằng cách "biên dịch" địa chỉ giữa hai giao thức. NAT64 cho phép thiết bị IPv6 Only truy cập dịch vụ IPv4 Only và NAT46 ngược lại. Ưu điểm của Translation là đảm bảo khả năng tương thích ngược, cho phép triển khai IPv6 từng bước. Tuy nhiên, nó có thể làm tăng độ trễ, giảm hiệu suất và phá vỡ tính kết nối toàn tuyến.

06

6PE và 6VPE là gì và chúng được sử dụng như thế nào trong việc triển khai IPv6 trên mạng MPLS?

6PE (IPv6 Provider Edge) và 6VPE (IPv6 VPN Provider Edge) là các kỹ thuật đặc biệt được thiết kế để triển khai IPv6 trên mạng MPLS (Multiprotocol Label Switching). 6PE cho phép truyền tải gói tin IPv6 qua các LSP (Label Switched Path) chạy IPv4 Only mà không cần nâng cấp mạng lõi. 6VPE mở rộng 6PE để hỗ trợ dịch vụ VPN IPv6 trên mạng MPLS, cho phép xử lý đồng thời cả lưu lượng IPv4 VPN và IPv6 VPN. Các kỹ thuật này giúp các nhà cung cấp dịch vụ triển khai IPv6 một cách hiệu quả trên hạ tầng MPLS hiện có.

07

Tài liệu hướng dẫn xây dựng kế hoạch chuyển đổi IPv6 cho cơ quan, đơn vị thực hiện theo những giai đoạn nào

VNNIC đã xây dựng tài liệu, cẩm nang lập kế hoạch chuyển đổi IPv6 cho cơ quan nhà nước, được nhân rộng cho khối đơn vị, doanh nghiệp có mạng sử dụng IP/ASN độc lập, bao gồm ba giai đoạn chính thức: Giai đoạn 1: Chuẩn bị (đào tạo nhân sự, rà soát hạ tầng, đăng ký địa chỉ IPv6); Giai đoạn 2: Kết nối và thử nghiệm (kết nối IPv6 với Internet, chuyển đổi ứng dụng, thử nghiệm dịch vụ IPv6); và Giai đoạn 3: Chuyển đổi chính thức (mở rộng triển khai IPv6, chuyển đổi toàn bộ mạng lưới, hướng tới IPv6 Only). Lộ trình này nhấn mạnh cả yếu tố kỹ thuật và các hoạt động chuẩn bị về nhân lực, truyền thông.

08

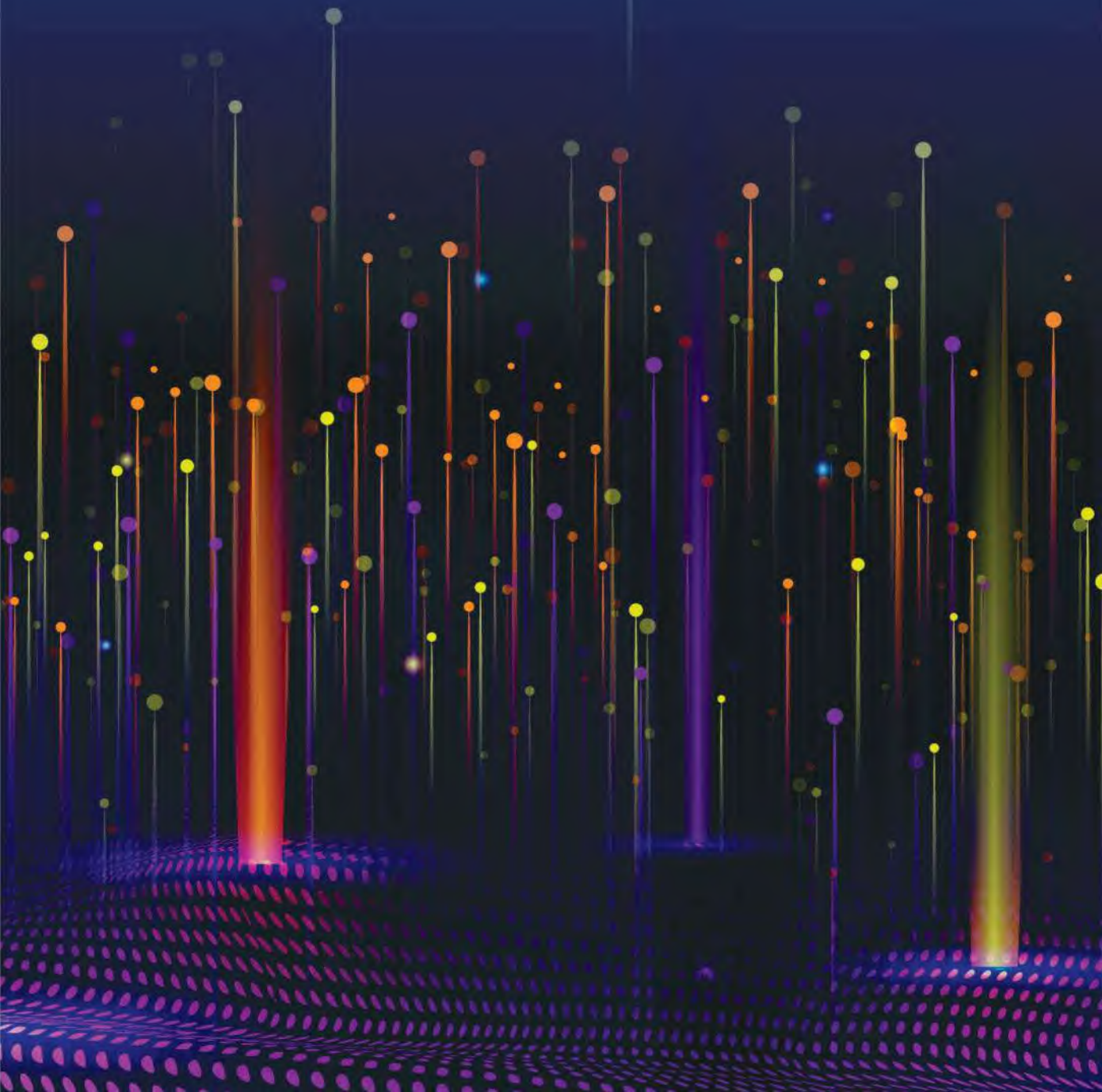
Việc lựa chọn kỹ thuật chuyển đổi IPv4 sang IPv6 cần dựa trên những yếu tố nào?

Việc lựa chọn kỹ thuật chuyển đổi IPv4 sang IPv6 cần dựa trên nhiều yếu tố quan trọng như đặc thù hệ thống mạng của tổ chức, quy mô, công nghệ hiện tại, loại hình dịch vụ, chi phí dự kiến, yêu cầu về hiệu suất, tính ổn định, các vấn đề bảo mật và mục tiêu dài hạn trong quá trình chuyển đổi. Việc cân nhắc kỹ lưỡng các yếu tố này sẽ giúp đảm bảo quá trình chuyển đổi diễn ra suôn sẻ, hiệu quả và tiết kiệm chi phí.

PHẦN 1 – LÝ THUYẾT

CHƯƠNG 6

CÁC KỸ THUẬT TRIỂN KHAI IPv6 ONLY



CHƯƠNG 6

CÁC KỸ THUẬT TRIỂN KHAI IPv6 ONLY

IPv6 Dual Stack là phương án an toàn, được khuyến cáo và sử dụng nhiều nhất trong việc chuyển đổi các hệ thống mạng sang IPv6 nhưng đó chỉ là bước trung gian để hướng đến mục tiêu cuối cùng IPv6 Single Stack hay IPv6 Only. Hiện nay mạng Internet vẫn tồn tại nhiều hệ thống IPv4 Only, chúng ta không thể chờ mạng Internet chuyển hoàn toàn sang Dual Stack rồi mới chuyển hệ thống của mình Single-Stack. Vì thế thách thức lớn nhất đối với IPv6 Only là vẫn cần truy cập các hệ thống IPv4 Only. Để giải quyết vấn đề này, chúng ta có thể sử dụng các giải pháp kỹ thuật như NAT64/DNS64, DS-Lite và 464XLAT, tuy nhiên các giải pháp này vẫn tồn tại những hạn chế nhất định và có thể gây ra vấn đề tương thích ứng dụng. Mặc dù mục tiêu dài hạn là đơn giản hóa quản lý nhưng giai đoạn đầu triển khai IPv6 Only có thể phức tạp và đòi hỏi sự chuẩn bị kỹ lưỡng về mặt kỹ thuật.

Chương 6 tập trung đặc biệt vào các kỹ thuật triển khai mô hình IPv6 Only. Chương này trình bày lý do và lợi ích của việc chuyển đổi hoàn toàn sang IPv6, nhấn mạnh đây là một xu hướng tất yếu để giải quyết vấn đề cạn kiệt địa chỉ IPv4 và tối ưu hóa mạng. Phần lớn nội dung sau đó đi sâu vào giới thiệu và giải thích chi tiết các giải pháp kỹ thuật như DNS64/NAT64, DS-Lite và 464XLAT, là những công cụ then chốt để các hệ thống IPv6 Only vẫn có thể tương tác với hạ tầng IPv4 hiện tại một cách hiệu quả.

Những nội dung chi tiết của chương này gồm:

Bạn sẽ hiểu được rằng **IPv6 Only là mục tiêu cuối cùng** và là xu hướng tất yếu trong quá trình chuyển đổi mạng, nhằm giải quyết tình trạng cạn kiệt IPv4 và tối ưu hóa hiệu suất.

Bạn sẽ nắm bắt được các **lợi ích quan trọng khi chuyển đổi sang IPv6 Only**.

Bạn sẽ được cung cấp thông tin về các **chính sách và công nghệ đang thúc đẩy việc triển khai IPv6 Only**.

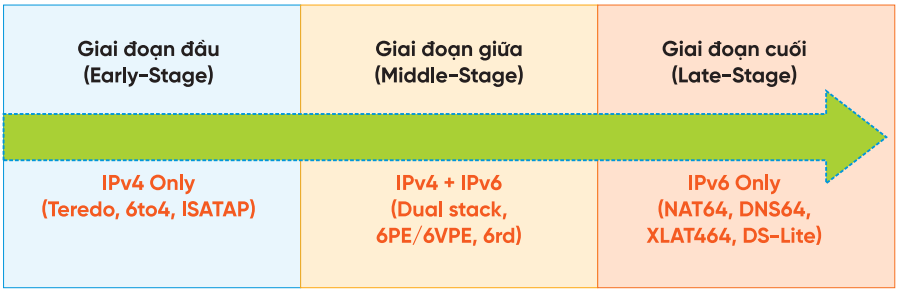
Bạn sẽ được giới thiệu về **IPv6+ (IPv6-Enhanced)**, một khái niệm mới được xem là tương lai của IPv6 Only, nhằm đáp ứng các yêu cầu cao hơn của mạng Internet trong kỷ nguyên 5G, IoT và điện toán đám mây.

Bạn sẽ hiểu rõ về các **giải pháp kỹ thuật quan trọng để triển khai IPv6 Only**, bao gồm **DNS64/NAT64, Dual Stack Lite (DS-Lite) và 464XLAT.**

Chương này cũng cung cấp **các ví dụ** về việc triển khai thành công IPv6 Only trên thế giới.

6.1. GIỚI THIỆU VỀ IPv6 ONLY VÀ CÁC GIAI ĐOẠN CHUYỂN ĐỔI

Có ba giai đoạn cho việc chuyển đổi từ IP4 sang sử dụng hoàn toàn IPv6. Những giải pháp đề cập ở chương 5 thường được triển khai trong giai đoạn Middle-Stage như hình mô tả bên dưới. Các chuyên gia không mong muốn giai đoạn này kéo dài lâu mà cần nhanh chóng chuyển sang giai đoạn Late-Stage, chỉ sử dụng duy nhất giao thức IPv6. IPv6 Only là mô hình mạng hiện đại trong đó toàn bộ hệ thống hoạt động với một mình giao thức IPv6, loại bỏ hoàn toàn sự phụ thuộc vào IPv4. Đây là xu hướng tất yếu nhằm giải quyết tình trạng cạn kiệt địa chỉ IPv4, đồng thời đơn giản hóa việc quản lý mạng và tối ưu hóa về hiệu suất hoạt động.



Hình 90. Các giai đoạn chuyển đổi từ IPv4 sang IPv6

Không chỉ vậy, IPv6 Only còn hỗ trợ rất tốt cho các công nghệ tiên tiến như IoT, 5G và điện toán đám mây. Vì thế, các tổ chức lớn như Google, Facebook, LinkedIn và Microsoft đã triển khai mô hình IPv6 Only trên hạ tầng của họ, đặc biệt cho các trung tâm dữ liệu. Các nhà cung cấp dịch vụ di động lớn như T-Mobile (Mỹ), Jio (Ấn Độ), Sunrise (Thụy Sĩ), SK Telecom (Hàn Quốc), Telstra (Úc), NTT DOCOMO (Nhật Bản) cũng đã áp dụng IPv6 Only cho mạng 4G/5G. Tại Mỹ, chính phủ đã yêu cầu tất cả cơ quan công quyền hoàn thành ít nhất 80% kế hoạch triển khai IPv6 Only cho hệ thống của mình vào cuối năm 2025. Chính phủ Trung Quốc cũng đã lập kế hoạch chuyển hoàn toàn các hệ thống mạng trong nước sang sử dụng IPv6 Only vào cuối năm 2030.

IPv6 Only là bước tiến chiến lược trong quá trình hiện đại hóa mạng, chuẩn bị cho sự phát triển mạnh mẽ của thế hệ Internet mới. Đây cũng là cách tốt nhất và duy nhất để loại bỏ những hạn chế của IPv4, đồng thời khai thác những tính năng ưu việt của IPv6.

6.2. LỢI ÍCH KHI CHUYỂN ĐỔI SANG IPv6 ONLY

Mô hình Dual Stack từng được coi là giải pháp chuyển đổi hiệu quả so với Tunneling và Translation nhưng nó không bền vững trong dài hạn vì vẫn còn duy trì sự tồn tại của IPv4. IPv6 Only là được xem là phương án triệt để, bền vững và tối ưu nhất để chuyển mạng Internet sang một giai đoạn phát triển mới. Thời điểm này cũng chín muồi để chuyển đổi sang IPv6 Only vì phần lớn ứng dụng, công nghệ và hạ tầng hiện đại đã sẵn sàng cho IPv6. Sau đây là những lợi ích, những điểm tối ưu mà IPv6 Only lại:

Chấm dứt hoàn toàn sự phụ thuộc vào IPv4

Việc duy trì mô hình Dual Stack khiến hệ thống vẫn phụ thuộc vào địa chỉ IPv4, trong khi tài nguyên IPv4 đã cạn kiệt và ngày càng khan hiếm. Điều này hạn chế khả năng mở rộng hạ tầng mạng và tạo áp lực về chi phí cho địa chỉ IPv4. Nếu chuyển sang IPv6 Only thì tất cả những hạn chế của IPv4 sẽ được giải quyết hoàn toàn và ngay lập tức, đồng thời cho phép mạng lưới mở rộng mà không gặp vấn đề.

Đơn giản hóa công tác vận hành và quản lý hệ thống

Dual Stack đòi hỏi quản lý song song cả hai giao thức IPv4 và IPv6, làm tăng sự phức tạp trong quy hoạch, giám sát, xử lý sự cố và bảo trì mạng. Chuyển sang IPv6 Only giúp giảm đáng kể khối lượng công việc vì các kỹ sư mạng chỉ tập trung vào một giao thức duy nhất. Các sai sót trong vận hành khai thác cũng được giảm thiểu.

Tối ưu hóa tài nguyên và hiệu suất hệ thống

Khi loại bỏ IPv4, các thiết bị mạng không còn duy trì bảng định tuyến kép và các giao thức, dịch vụ đi kèm với IPv4. Toàn bộ tài nguyên của thiết bị chỉ dành cho IPv6 nên hiệu suất hoạt động sẽ tăng lên và tốc độ xử lý nhanh hơn.

Cải thiện khả năng bảo mật

Thay vì quản lý bảo mật cho cả IPv4 và IPv6 thì công tác bảo mật chỉ tập trung vào IPv6, giảm thiểu gánh nặng quản lý và xây dựng các chính sách bảo mật. Các vấn đề bảo mật liên quan đến IPv4 được loại bỏ và cơ chế bảo mật của IPv6 sẽ được phát huy.

Sẵn sàng cho sự phát triển Internet thế hệ mới

Không chỉ giải quyết các vấn đề hiện tại mà IPv6 Only còn đặt nền móng vững chắc cho sự phát triển của thế hệ mạng Internet tiếp theo, khi mà IPv4 trở nên lỗi thời và không thể đáp ứng yêu cầu của các công nghệ như IoT, 5G/6G, Blockchain, A.I và các dịch vụ mới khác.

6.3. CÁC CHÍNH SÁCH, CÔNG NGHỆ VỀ IPv6 ONLY

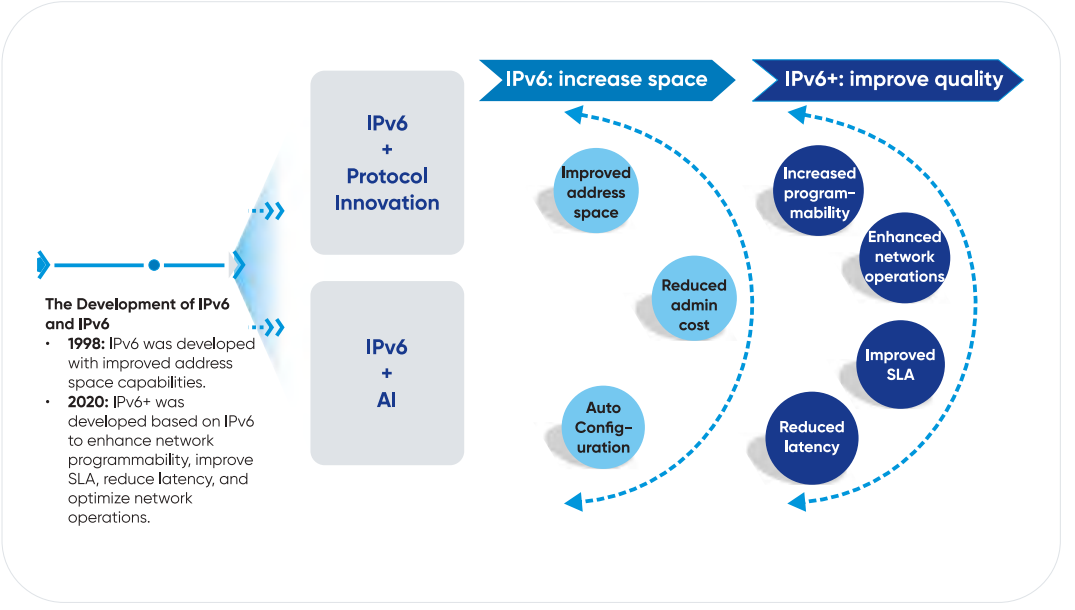
Ngoài những lợi ích về mặt kỹ thuật nêu trên thì một số chính sách cũng góp phần thúc đẩy việc triển khai IPv6 Only. Một trong những chính sách lớn đã được thông báo từ Tiểu ban kiến trúc Internet IAB vào tháng 11/2016, trong đó yêu cầu các công nghệ và giao thức mới sẽ không còn hỗ trợ IPv4 nữa mà chỉ tập trung cho IPv6. Việc này khuyến khích các tổ chức và nhà phát triển chuyển sang sử dụng IPv6 để đảm bảo khả năng phát triển bền vững của mạng Internet tương lai.

Cũng vào tháng 6/2016, Apple đã đưa ra quy định yêu cầu tất cả các ứng dụng đăng ký trên App Store phải hỗ trợ IPv6 Only, đánh dấu bước tiến quan trọng trong thúc đẩy áp dụng IPv6 trên các nền tảng di động. Điều này bảo đảm các ứng dụng hoạt động tốt khi thiết bị di động chuyển sang hoạt động với IPv6 Only, đồng thời yêu cầu các nhà phát triển tuân theo xu hướng này.

Về mặt công nghệ, nhiều giải pháp, nền tảng mới hiện nay chỉ hoạt động với IPv6. Ví dụ, SRv6 (Segment Routing over IPv6) là công nghệ cung cấp cách thức định tuyến hiện đại, hiệu quả và linh hoạt. Các giải pháp IoT như Matter và Thread cũng được thiết kế để hoạt động chỉ trên IPv6, giúp cải thiện khả năng kết nối và quản lý các thiết bị IoT và mạng cảm biến dân dụng. Theo khuyến cáo của 3GPP (3rd Generation Partnership Project) các mạng 5G Standalone (SA) nên chuyển sang hoạt động với IPv6 Only để tối ưu hóa khả năng kết nối, bảo mật và hiệu suất. Những điều này cho thấy rõ sự không thể thiếu của IPv6 trong các công nghệ tương lai.

6.4. IPv6+ TƯƠNG LAI CỦA IPv6 ONLY

Không dừng lại ở IPv6 Only vào năm 2020, một khái niệm mới của IPv6 đã ra đời đó là IPv6+ hay IPv6-Enhanced. IPv6+ là sự mở rộng của IPv6, được thiết kế để đáp ứng các yêu cầu ngày càng cao của hệ thống mạng trong thời kỳ bùng nổ các công nghệ như 5G, IoT và điện toán đám mây. Trong khi IPv6 giúp mở rộng không gian địa chỉ, tối ưu hoạt động và nâng cao hiệu suất mạng thì IPv6+ kết hợp với những công nghệ mới sẽ nhắm tới mục tiêu đơn giản hóa công tác vận hành, cải thiện chất lượng mạng (SLA), giảm thiểu độ trễ mạng và tăng cường khả năng lập trình mạng.



Hình 91. Đặc điểm và lợi ích của IPv6+ (nguồn: Roland Berger)

6.4.1. Đặc điểm nổi bật của IPv6+

IPv6+ mang lại những cải tiến quan trọng trong quản lý mạng và tối ưu hóa các dịch vụ, dưới đây là một số đặc điểm nổi bật của IPv6+:

Tối ưu hóa hiệu suất mạng

IPv6+ giúp giảm độ trễ và tối ưu hóa việc truyền tải dữ liệu qua mạng, ví dụ, với việc áp dụng **Segment Routing (SRv6)**, một trong những công nghệ của IPv6+, các gói tin có thể được định tuyến một cách thông minh và linh hoạt, giúp tăng cường khả năng sử dụng băng thông và giảm thiểu độ trễ, điều này rất quan trọng đối với các dịch vụ đòi hỏi băng thông lớn như video HD hay VR (Virtual Reality).

Hỗ trợ cho các công nghệ mạng hiện đại

IPv6+ tích hợp các công nghệ như **Network Slicing**, cho phép tách hệ thống mạng thành các phần riêng biệt, giúp tối ưu hóa việc phân phối tài nguyên và cải thiện hiệu suất cho các ứng dụng khác nhau. Một ví dụ điển hình là trong mạng 5G, khi các phần của mạng có thể được điều chỉnh và tối ưu hóa cho từng loại dịch vụ, chẳng hạn như cho việc kết nối các thiết bị IoT hoặc kết nối với người dùng di động.

Tăng cường khả năng lập trình mạng

IPv6+ mang lại khả năng tự động hóa cao hơn nhờ vào các cơ chế như **AI-driven Networking** (mạng điều khiển bằng AI). Điều này giúp các mạng có thể tự học và tự điều chỉnh các cấu hình để tối ưu hóa hiệu suất mà không cần sự can thiệp của con người. Ví dụ, các trung tâm dữ liệu có thể tự động điều chỉnh lưu lượng mạng dựa trên nhu cầu thực tế, giúp giảm chi phí và nâng cao hiệu quả vận hành.

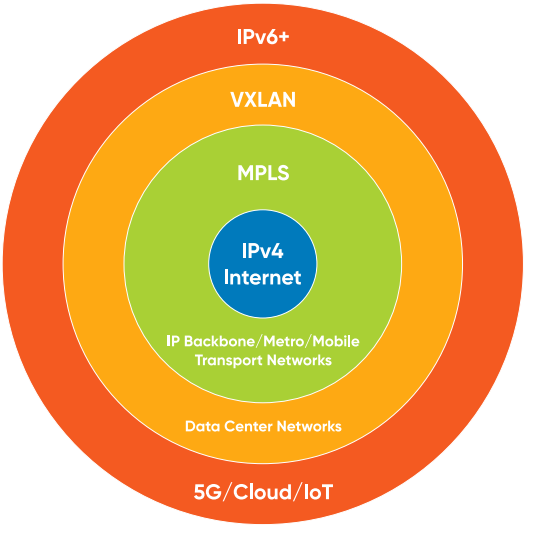
Tiết kiệm năng lượng và bảo vệ môi trường

IPv6+ cũng hỗ trợ các giải pháp "mạng xanh", giúp giảm mức độ tiêu thụ năng lượng trong các trung tâm dữ liệu và mạng, điều này rất quan trọng trong bối cảnh hiện nay khi các tổ chức đang cố gắng giảm thiểu dấu vết carbon và tiết kiệm tài nguyên. Công nghệ như **Green Networking** giúp tối ưu hóa cách thức truyền tải dữ liệu và sử dụng băng thông, dẫn đến tiết kiệm năng lượng đáng kể.

6.4.2. Ứng dụng thực tế

IPv6+ đã được triển khai bởi nhiều nhà cung cấp dịch vụ và tổ chức lớn trên toàn cầu. Ví dụ, China Mobile đã áp dụng SRv6 để cải thiện chất lượng mạng và hỗ trợ triển khai 5G với khả năng tự động hóa cao. Swisscom, một nhà mạng lớn tại châu Âu, cũng đã ứng dụng IPv6+ trong hạ tầng mạng của mình để tối ưu hóa lưu lượng và nâng cao SLA. Các hệ thống mạng quy mô lớn, như giao thông thông minh hoặc thành phố thông minh, cũng đang tích hợp IPv6+ để tăng hiệu quả vận hành và quản lý.

Như vậy, IPv6+ được xem là bản nâng cấp của IPv6 nhằm đổi mới các hệ thống mạng IP, hướng đến kỷ nguyên 5G, Cloud và IoT. Việc chuyển sang IPv6 Only sẽ là tiền đề để triển khai các giải pháp IPv6+.



Hình 92. IPv6+ hỗ trợ tốt cho 5G/Cloud/IoT

6.5. GIẢI PHÁP KỸ THUẬT CHO IPv6 ONLY

Để triển khai mạng IPv6 Only, các giải pháp kỹ thuật đóng vai trò quan trọng trong việc đảm bảo khả năng kết nối với các dịch vụ và hạ tầng vẫn dựa trên IPv4. Một số công nghệ chính bao gồm NAT64/DNS64, giúp thiết bị IPv6 Only truy cập tài nguyên IPv4 thông qua cơ chế chuyển đổi và phân giải địa chỉ; 464XLAT, hỗ trợ các ứng dụng IPv4 Only hoạt động trên mạng IPv6 và DS-Lite giúp triển khai IPv6 Only mạng truy cập cố định kết hợp với CGNAT. Những giải pháp này giúp chuyển đổi linh hoạt, đáp ứng nhu cầu đa dạng của nhà mạng và doanh nghiệp.

Nhiều doanh nghiệp và nhà mạng trên thế giới đã triển khai thành công mô hình IPv6 Only. Ví dụ, nhà cung cấp dịch vụ viễn thông T-Mobile ở Mỹ đã chuyển sang IPv6 Only cho mạng di động của mình từ năm 2018, kết hợp với giải pháp DNS64 và NAT64 để hỗ trợ truy cập IPv4. Tại Nhật Bản, NTT Docomo đã triển khai IPv6 Only cho các dịch vụ di động, sử dụng các công nghệ như 464XLAT. Một ví dụ điển hình khác là **Comcast** (Mỹ), đã áp dụng **DS-Lite** để cung cấp dịch vụ IPv6 trong khi vẫn duy trì kết nối IPv4 cho khách hàng của mình. Các công ty như **Meta** và **Google** cũng đã thử nghiệm triển khai IPv6 Only trong các trung tâm dữ liệu, sử dụng các công nghệ như **NAT64** và **DNS64** để kết nối với các dịch vụ IPv4. Những ví dụ này cho thấy các giải pháp kỹ thuật như NAT64/DNS64, 464XLAT và DS-Lite để triển khai IPv6 Only một cách hiệu quả trong cả môi trường di động lẫn cố định.

ISP (name)	Country	Transition Mechanism (NAT64/464xlat, 6rd, DS-Lite, Dual Stack, ...)	Network Type (mobile, DSL, fiber, cable, satellite,...)
	DK,NO	6RD	Fibre
	US	6rd	AT&T Old PPPoE ADSL
	US	Native IPv6 (Dual Stack)	802.1x "IPDSL" over
	CH	DS-Lite	DOCSIS
	US	Dual Stack MAP-T (EFT)	DOCSIS
	US	dual stack	DOCSIS
	CR	Dual-stack	Docsis, Fiber, GPON
	DE	Dual Stack	dsl/vdsl
	IE	dual stack	VDSL2 & FTTH
	GR	Dual-Stack, DS-Lite	DSL
	NO	Dual stack	DOCSIS
	TW	Dual stack	VDSL, FTTH
		dual stack, DS-Lite	fibre?
	DE	DS-Lite	DOCSIS
	DE	Dual Stack and NAT64	WIFI
	DE	DS-Lite	DSL/FTTB
	MA	Dual-Stack	Fiber
	UA	dual stack	fibre, ETTH
	DE	Dual Stack	DSL
	CZ	DS-Lite	DSL
	ES	dual stack, DS-Lite	fibre
	FR	Dual-stack	ADSL, VDSL, Fibre
	PL	DS-Lite	DSL and fibre
	SK	DS-Lite	DSL
	GR	Dual-stack / lw4o6	xDSL
	BE	dual stack	DSL
	DE	DS-Lite	DOCSIS

Hình 93. Các công nghệ cho IPv6 Only đối với Internet băng rộng cố định

Country	Transition Mechanism (NAT64/464xlat, 6rd, DS-Lite, Dual Stack, ...)	Network Type (mobile, DSL, fiber, cable, satellite,...)
US	?	Mobile
BT	Dual Stack	Mobile
GB	464XLAT	Mobile
TT	Dual Stack	Mobile
DE	464XLAT, NAT64	mobile (2G,3G,4G)
DE	Dual Stack	mobile (2G,3G,4G)
EE	dual stack	mobile
TW	Dual Stack	Mobile
VN	dual stack	LTE
NO	Dual stack	3GPP
FR	Dual-stack	Mobile
PL	464XLAT	Mobile
IN	464XLAT	Mobile
CA	NAT64/464XLAT	Wireless
US	464XLAT	mobile
US	464XLAT, NAT64	mobile
SE	Dual stack	3GPP
AU	464XLAT	mobile

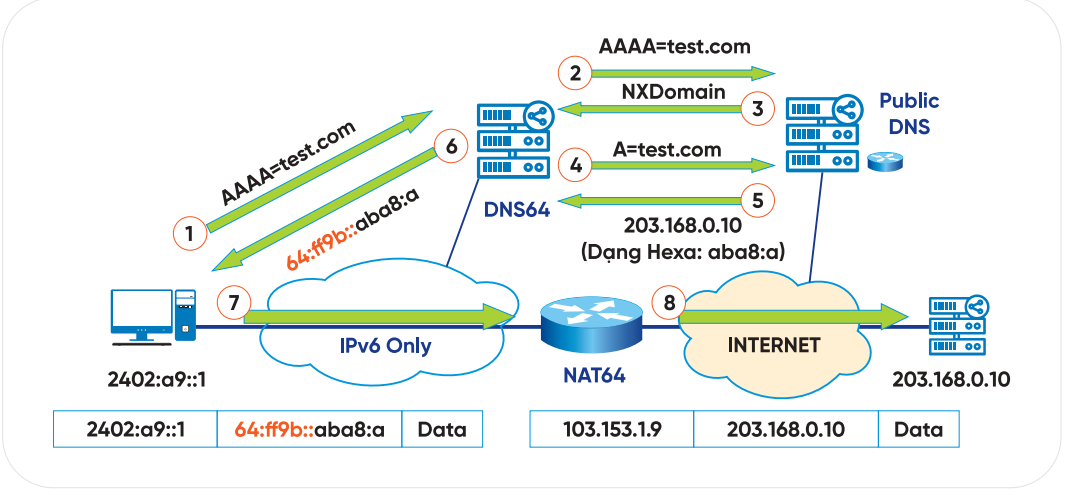
Hình 94. Các công nghệ cho IPv6 Only đối với Internet băng rộng di động

6.6. KỸ THUẬT DNS64/NAT64

Giải pháp **DNS64**/**NAT64** là một kỹ thuật phổ biến để triển khai môi trường **IPv6 Only**, đặc biệt trong các trung tâm dữ liệu và mạng người dùng doanh nghiệp. Giải pháp này được áp dụng nhanh chóng, không yêu cầu thay đổi cấu trúc mạng hoặc ứng dụng hiện tại nhờ khả năng hỗ trợ IPv6 hiệu quả.

DNS64 Server đóng vai trò phân giải tên miền và can thiệp vào kết quả trả về cho DNS Client. Khi một thiết bị **IPv6 Only** gửi yêu cầu phân giải tên miền (bản ghi AAAA) đến DNS64, server sẽ truy vấn địa chỉ IPv6 từ hệ thống DNS bên ngoài. Nếu không nhận được địa chỉ IPv6, DNS64 sẽ chuyển sang truy vấn địa chỉ IPv4 (bản ghi A). Sau khi nhận được địa chỉ IPv4, DNS64 Server chuyển đổi địa chỉ này sang định dạng Hexadecimal, kết hợp với **NAT64 Prefix** được định sẵn để tạo ra địa chỉ IPv6 tích hợp, sau đó trả về cho thiết bị.

Ví dụ, với tên miền có địa chỉ IPv4 là **203.168.0.10**, DNS64 sẽ tạo bản ghi AAAA là **64:FF9B::ABA8:A**, trong đó **64:FF9B::** là NAT64 Prefix và **ABA8:A** là giá trị Hexadecimal của địa chỉ IPv4.



Hình 95. Nguyên tắc hoạt động của DNS64 và NAT64

Thiết bị NAT64 có nhiệm vụ chuyển đổi địa chỉ IPv6 của các gói tin thành IPv4 trước khi gửi ra ngoài Internet. Chỉ cần chuyển đổi địa chỉ IPv6 nguồn sang IPv4 còn địa chỉ IPv6 đích là địa chỉ do DNS64 tích hợp từ IPv4 ở bước trên nên chỉ cần trả lại địa chỉ IPv4 đích ban đầu. Việc này sẽ được thực hiện ngược lại khi gói tin được trả về. Như vậy, với kỹ thuật NAT64 thì các thiết bị hoặc ứng dụng IPv6 có thể truy cập thiết bị IPv4 bình thường mà không cần phải thay đổi thiết bị mạng hoặc ứng dụng. Điều này rất đơn giản và thuận tiện, không cần phải duy trì giao thức IPv4 bên trong mạng, chỉ cần dãy IPv4 trên thiết bị NAT64 phục vụ cho nhu cầu truy cập đến thiết bị IPv4 bên ngoài.

Tổng thể quá trình kết hợp giữa hai kỹ thuật này như sau:

Yêu cầu truy cập: Thiết bị IPv6 muốn truy cập một trang web có địa chỉ IPv4, ví dụ test.com.

Truy vấn DNS: Thiết bị IPv6 gửi yêu cầu phân giải tên miền test.com đến máy chủ DNS64.

DNS64 tạo bản ghi AAAA giả: DNS64 kiểm tra xem test.com có bản ghi AAAA (bản ghi IPv6) hay không. Nếu không có, DNS64 sẽ tìm bản ghi A (bản ghi IPv4). Giả sử bản ghi A của test.com là 203.168.0.10. DNS64 sẽ tạo ra một bản ghi AAAA tích hợp, ví dụ 64:FF9B::ABA8:A như đã trình bày ở phần trước.

Trả lời DNS: DNS64 trả về bản ghi AAAA tích hợp (64:FF9B::ABA8:A) cho thiết bị IPv6.

Gửi gói tin IPv6: Thiết bị IPv6 nhận được địa chỉ IPv6 và gửi gói tin đến địa chỉ đích 64:FF9B::ABA8:A.

Xử lý tại NAT64: Router NAT64 nhận gói tin IPv6 này. Do địa chỉ đích bắt đầu bằng NAT64 Prefix 64:FF9B:: nên Router biết cần phải thực hiện chuyển đổi các địa chỉ nguồn và đích sang IPv4.

Chuyển đổi sang IPv4: Router NAT64 trích xuất 32 bit cuối của địa chỉ IPv6 đích (ABA8:A), chuyển đổi nó trở lại dạng thập phân (203.168.0.10). Địa chỉ IPv6 nguồn được đổi thành địa chỉ IPv4 của chính Router NAT64 hoặc thuộc dãy IPv4 được khai báo riêng.

Gửi gói tin IPv4: Router NAT64 gửi gói tin IPv4 đến máy đích 203.168.0.10.

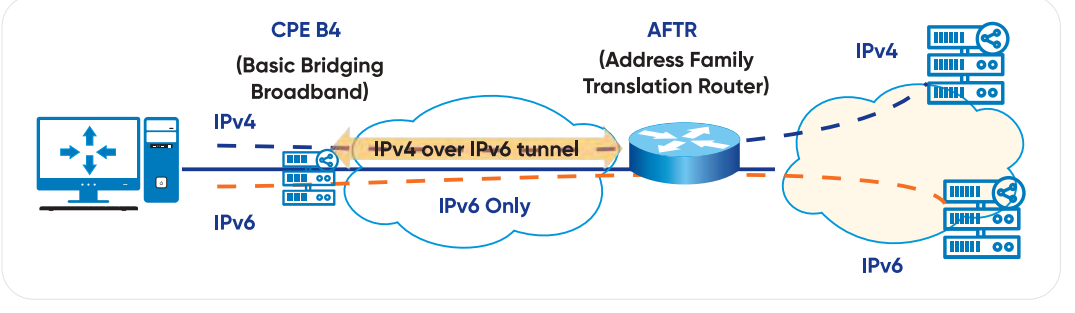
Nhận và xử lý phản hồi: Máy chủ 203.168.0.10 nhận gói tin và gửi phản hồi trở lại router NAT64 dưới dạng gói tin IPv4.

Chuyển đổi trở lại IPv6: Router NAT64 nhận gói tin IPv4 phản hồi sẽ chuyển đổi địa chỉ nguồn IPv4 (là địa chỉ đích ban đầu) thành địa chỉ IPv6 tương ứng (sử dụng tiền tố 64:FF9B::96) và gửi gói tin IPv6 trở lại thiết bị IPv6 ban đầu.

Như vậy sự kết hợp giữa DNS64 và NAT64 mang lại một giải pháp hiệu quả và linh hoạt cho phép các thiết bị IPv6 truy cập tài nguyên IPv4 một cách liền mạch và trong suốt. Đây là một giải pháp lý tưởng cho việc triển khai mạng IPv6 Only đối với hệ thống mạng của các doanh nghiệp. Tuy nhiên giải pháp này cũng có một số hạn chế như một số ứng dụng gặp vấn đề khi hoạt động với NAT64 và phụ thuộc vào DNS64.

6.7. KỸ THUẬT DUAL STACK LITE (DS LITE)

DS-Lite là một giải pháp thông minh và hiệu quả giúp các ISP chuyển đổi sang IPv6 Only một cách nhanh chóng trong khi vẫn đảm bảo trải nghiệm khả năng truy cập tới các dịch vụ IPv4 trên Internet.



Hình 96. Nguyên tắc hoạt động của giải pháp DS-Lite

Các thành phần chính trong kiến trúc DS-Lite gồm:

CPE 4B (Basic Bridging Broadband)

CPE B4 là thiết bị đầu cuối tại phía người dùng, đóng vai trò kết nối các thiết bị mạng nội bộ (LAN) với hạ tầng mạng IPv6 của nhà cung cấp dịch vụ. Thiết bị này cung cấp địa chỉ IPv4 Private và IPv6 cho các thiết bị trong mạng nội bộ. Đồng thời, CPE B4 thiết lập một đường hầm (IPv4 over IPv6 Tunnel) đến router AFTR. Tất cả lưu lượng IPv4 từ mạng nội bộ được đóng gói (Encapsulate) bằng IPv6 và truyền qua đường hầm này, cho phép các thiết bị IPv4 truy cập thông qua mạng IPv6 Only của ISP.

AFTR (Address Family Transition Router)

AFTR là một thành phần cốt lõi trong kỹ thuật DS-Lite được đặt tại nhà mạng. Đây là điểm cuối của đường hầm IPv6, chịu trách nhiệm mở gói (De-Encapsulate) IPv6 để lấy lại gói tin IPv4 gửi từ CPE B4. Ngoài ra, AFTR thực hiện một nhiệm vụ quan trong khác là NAT44 (Network Address Translation), chuyển đổi địa chỉ nguồn IPv4 Private thành IPv4 Public rồi chuyển tiếp ra mạng IPv4 đích. Khi nhận phản hồi từ mạng IPv4, AFTR đóng gói gói tin IPv4 vào gói IPv6 và chuyển tiếp lại cho thiết bị người dùng qua đường hầm.

Sau đây là chi tiết quá trình hoạt động của DS-Lite bao gồm các bước sau:

Bước 1: Một thiết bị từ khách hàng muốn truy cập trang web IPv4. Yêu cầu này được gửi tới CPE B4.

Bước 2: CPE B4 đóng gói tin IPv4 vào trong gói tin IPv6, địa chỉ IPv6 nguồn là của của CPE B4 và IPv6 đích là của AFTR.

Bước 3: Gói IPv6 được chuyển qua mạng IPv6 của nhà cung cấp dịch vụ đến AFTR.

Bước 4: AFTR giải mã gói IPv6 để lấy gói IPv4 bên trong. Gói tin IPv4 này sau đó được NAT44 sang địa chỉ IPv4 Public, cho phép kết nối đến máy chủ IPv4 đích.

Bước 5: Máy chủ web gửi gói tin phản hồi (IPv4) về địa chỉ IP Public của AFTR.

Bước 6: Gói tin IPv4 được AFTR đóng gói lại thành gói tin IPv6 và gửi qua mạng IPv6 Only của ISP về CPE B4.

Bước 7: CPE B4 mở gói tin IPv6 lấy lại gói IPv4 và chuyển tiếp đến thiết bị nội bộ tương ứng.

Có thể nói DS-Lite là một giải pháp rất hiệu quả và đơn giản giúp các nhà mạng chuyển sang hoạt động với IPv6 Only. Nhờ vai trò của các thành phần như CPE B4 và AFTR, giải pháp DS-Lite đảm bảo khả năng tương thích ngược với IPv4 và giúp giảm thiểu sự phụ thuộc vào địa chỉ IPv4 đang cạn kiệt. Mặc dù vậy, DS-Lite cũng có một số hạn chế cần lưu ý. Đầu tiên, nó phụ thuộc vào NAT44 tại AFTR, có thể dẫn đến giới hạn kết nối đồng thời do giới hạn số lượng cổng TCP/UDP nếu số lượng khách hàng lớn. Thứ hai, quá trình đóng và giải đóng gói IPv4-over-IPv6 tại CPE và AFTR làm tăng độ trễ, ảnh hưởng đến dịch vụ thời gian thực như VoIP. Cuối cùng, việc triển khai yêu cầu đầu tư cơ sở hạ tầng và tối ưu hóa quy trình vận hành để đạt hiệu quả tối đa.

6.8. KỸ THUẬT 464XLAT

Trong một số trường hợp, kỹ thuật DNS64/NAT64 không thể sử dụng được. Ví dụ, một số ứng dụng sử dụng trực tiếp địa chỉ IPv4 (Literal) thay vì tên miền, khiến DNS64 không thể hoạt động. Đối với mạng di động, khi điện thoại trở thành điểm phát WiFi (Hotspot) nó chỉ cấp địa chỉ IPv4 cho các thiết bị khác, dẫn đến NAT64 không thể xử lý vì địa chỉ nguồn của các gói tin là IPv4.

Chính vì thế kỹ thuật 464XLAT được phát triển để giải quyết các hạn chế của DNS64/NAT64 và được sử dụng phổ biến trong lĩnh vực mạng di động. Các thiết bị di động IPv6 Only kết nối với dịch vụ IPv4 Only mà không gặp phải các vấn đề về tương thích. Nhiều nhà mạng di động lớn, ví dụ như T-Mobile, Verizon, đã áp dụng 464XLAT để cung cấp kết nối IPv6 cho khách hàng của mình.

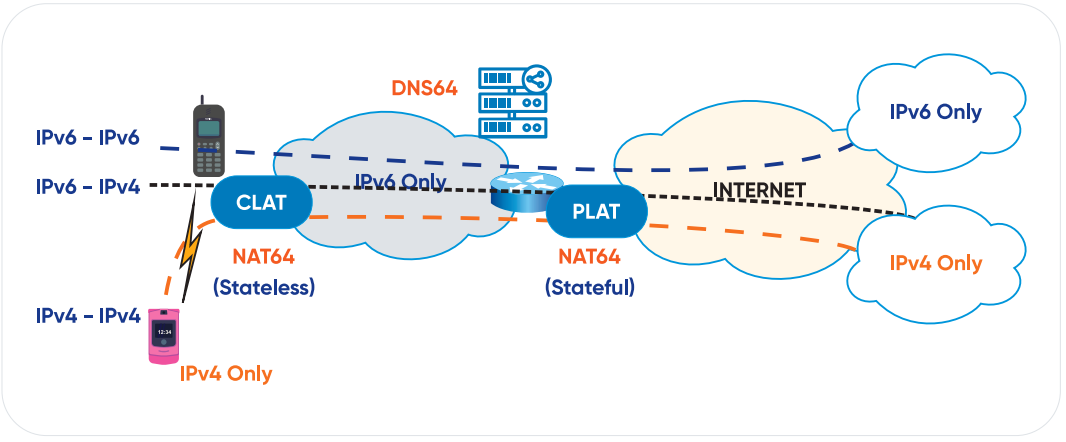
Trong mô hình kiến trúc của giải pháp 464XLAT mạng trục sẽ là IPv6 Only, còn việc xử lý các gói tin IPv4 được thực hiện tại hai thành phần chính:

CLAT (Customer Edge Translator):

CLAT là thành phần trong thiết bị người dùng có nhiệm vụ chuyển đổi địa chỉ IPv4 sang IPv6 và ngược lại (NAT46). Việc chuyển đổi này được thực hiện theo mô hình 1:1 nên được còn gọi là Stateless NAT.

PLAT (Provider Edge Translator):

PLAT là thành phần được triển khai ở nhà mạng, PLAT tiếp nhận các gói tin gửi từ CLAT và thực hiện chuyển đổi từ IPv6 sang IPv4 mới (NAT64). Việc chuyển đổi này theo mô hình N:1, trong đó nhiều địa chỉ nguồn IPv6 được ánh xạ với một địa chỉ IPv4 nên được gọi là Stateful NAT vì các thông tin của việc NAT cần được lưu lại.



Hình 97. Nguyên tắc hoạt động của giải pháp DS-Lite

Để hiểu hơn về hoạt động của 464XLAT, sau đây là mô tả chi tiết các loại kết nối thông qua hạ tầng IPv6 Only:

Kết nối từ IPv6 đến IPv6: Thiết bị đầu cuối trực tiếp sử dụng kết nối IPv6 mà không cần thông qua CLAT hay PLAT.

Kết nối từ IPv6 đến IPv4: CLAT chuyển đổi địa chỉ đích IPv4 thành địa chỉ IPv6 tích hợp (dựa trên NAT64 Prefix). DNS64 được sử dụng để thông báo NAT64 Prefix cho CLAT. Sau đó, PLAT sẽ thực hiện chuyển đổi gói tin IPv6 từ CLAT thành gói tin IPv4, bao gồm cả địa chỉ nguồn và đích.

Kết nối từ IPv4 đến IPv4: Với một dải địa chỉ IPv6 /64 được cung cấp cho thiết bị người dùng, CLAT trích xuất một phần /96 để chuyển đổi địa chỉ nguồn IPv4 Private thành địa chỉ IPv6. Đồng thời, địa chỉ đích IPv4 cũng được chuyển thành IPv6 qua NAT64 Prefix và gửi đến PLAT. PLAT sau đó chuyển đổi các gói tin IPv6 thành IPv4 hoàn chỉnh (nguồn và đích).

Có thể thấy, với 464XLAT các hệ thống IPv6 Only có thể kết nối với dịch vụ IPv4 Only rất hiệu quả. Trong giải pháp này, IPv4 Private được sử dụng tại CLAT còn IPv4 Public được sử dụng tại PLAT chỉ khi có kết nối đến dịch vụ IPv4 bên ngoài nên giúp giảm thiểu sự phụ thuộc vào tài nguyên IPv4 Public.

Chú ý:
- Hiện nay (2025) Windows vẫn chưa hỗ trợ CLAT cho kết nối Ethernet và Wifi dù Microsoft đã có thông báo sẽ triển khai tính năng này nên việc triển khai giải pháp 464XLAT cho mạng doanh nghiệp vẫn chưa khả thi. Các loại điện thoại phổ biến như Android và iOS đã hỗ trợ tốt CLAT.

6.9. TỔNG KẾT CHƯƠNG 6

Chương 6 đã tập trung phân tích về các kỹ thuật triển khai **IPv6 Only**, một xu hướng tất yếu trong sự phát triển của mạng Internet. Chương mở đầu với khái niệm IPv6 Only, mô tả các giai đoạn chuyển đổi cũng như những lợi ích khi loại bỏ hoàn toàn IPv4, giúp tối ưu hóa tài nguyên mạng và nâng cao hiệu suất hệ thống. Bên cạnh đó, chương 6 cũng đề cập đến các chính sách và công nghệ hỗ trợ triển khai IPv6 Only, đồng thời giới thiệu khái niệm **IPv6+**, được coi là tương lai của IPv6 Only với nhiều đặc điểm nổi bật.

Phần ứng dụng thực tế của chương 6 đã giới thiệu các giải pháp kỹ thuật quan trọng giúp triển khai IPv6 Only hiệu quả, bao gồm **DNS64/NAT64, Dual Stack Lite (DS Lite) và 464XLAT**, giúp đảm bảo tính tương thích với các hệ thống IPv4 hiện tại. Nhìn chung, chương 6 nhấn mạnh tầm quan trọng của việc chuyển đổi sang IPv6 Only trong bối cảnh IPv4 đang dần cạn kiệt, đồng thời cung cấp các giải pháp thực tiễn để các tổ chức và doanh nghiệp có thể triển khai IPv6 Only một cách tối ưu và bền vững.

6.10. CÂU HỎI ÔN TẬP CHƯƠNG 6

01

IPv6 Only là gì và tại sao nó được coi là mục tiêu cuối cùng trong quá trình chuyển đổi mạng?

IPv6 Only là mô hình mạng mà trong đó toàn bộ hệ thống chỉ sử dụng duy nhất giao thức IPv6, loại bỏ hoàn toàn sự phụ thuộc vào IPv4. Nó được coi là mục tiêu cuối cùng vì giải quyết triệt để tình trạng cạn kiệt địa chỉ IPv4, đơn giản hóa quản lý mạng, tối ưu hóa hiệu suất hoạt động và hỗ trợ tốt hơn cho các công nghệ tiên tiến như IoT, 5G và điện toán đám mây. Mặc dù Dual Stack là một bước an toàn và phổ biến trong quá trình chuyển đổi, nhưng nó vẫn duy trì sự tồn tại của IPv4, do đó không phải là giải pháp bền vững trong dài hạn.

02

Những lợi ích chính của việc chuyển đổi sang IPv6 Only là gì?

Việc chuyển đổi sang IPv6 Only mang lại nhiều lợi ích quan trọng, bao gồm:

- **Chấm dứt hoàn toàn sự phụ thuộc vào IPv4:** Giải quyết vấn đề cạn kiệt địa chỉ IPv4, cho phép mở rộng hạ tầng mạng mà không gặp rào cản về địa chỉ và chi phí liên quan đến IPv4.
- **Đơn giản hóa công tác vận hành và quản lý hệ thống:** Loại bỏ việc quản lý song song hai giao thức IPv4 và IPv6, giảm sự phức tạp trong quy hoạch, giám sát, xử lý sự cố và bảo trì mạng.
- **Tối ưu hóa tài nguyên và hiệu suất hệ thống:** Các thiết bị mạng không cần duy trì các bảng định tuyến và giao thức liên quan đến IPv4, giúp tăng hiệu suất hoạt động và tốc độ xử lý.
- **Cải thiện khả năng bảo mật:** Công tác bảo mật chỉ tập trung vào IPv6, giảm thiểu gánh nặng quản lý và loại bỏ các vấn đề bảo mật liên quan đến IPv4.
- **Sẵn sàng cho sự phát triển Internet thế hệ mới:** Đặt nền móng vững chắc cho các công nghệ tương lai như IoT, 5G/6G, Blockchain và AI, vốn đòi hỏi khả năng kết nối và địa chỉ lớn hơn IPv4 có thể cung cấp.

03

Những giai đoạn chính trong quá trình chuyển đổi từ IPv4 sang IPv6 được mô tả như thế nào?

Quá trình chuyển đổi từ IPv4 sang sử dụng hoàn toàn IPv6 thường được chia thành ba giai đoạn:

- **Early-Stage (Giai đoạn đầu):** Giai đoạn này chủ yếu tập trung vào việc triển khai IPv6 song song với IPv4 (Dual Stack) trên một số hệ thống và dịch vụ nhất định.
- **Middle-Stage (Giai đoạn giữa):** Giai đoạn này chứng kiến việc triển khai các kỹ thuật chuyển đổi như Tunneling và Translation (được đề cập ở chương 5). Dual Stack vẫn là phương án phổ biến trong giai đoạn này để đảm bảo khả năng tương thích.
- **Late-Stage (Giai đoạn cuối):** Đây là giai đoạn hướng tới mục tiêu IPv6 Only, trong đó các hệ thống và mạng lưới dần loại bỏ hoàn toàn IPv4. Các chuyên gia khuyến khích quá trình này diễn ra nhanh chóng để tận dụng tối đa lợi ích của IPv6.

04

Các giải pháp kỹ thuật nào được sử dụng để hỗ trợ việc triển khai mạng IPv6 Only trong khi vẫn đảm bảo khả năng truy cập các hệ thống IPv4?

Để triển khai mạng IPv6 Only mà vẫn đảm bảo khả năng truy cập các hệ thống IPv4, một số giải pháp kỹ thuật chính được sử dụng:

- **NAT64/DNS64:** Cho phép các thiết bị IPv6 Only truy cập tài nguyên IPv4 thông qua cơ chế chuyển đổi địa chỉ (NAT64) và phân giải tên miền (DNS64). DNS64 tạo ra các bản ghi AAAA (IPv6) tổng hợp từ bản ghi A (IPv4) và NAT64 chuyển đổi các gói tin IPv6 sang IPv4 và ngược lại.
- **Dual Stack Lite (DS-Lite):** Giúp các ISP chuyển đổi sang IPv6 Only trong khi vẫn cung cấp khả năng truy cập IPv4 cho người dùng cuối thông qua việc đóng gói các gói tin IPv4 trong IPv6 (IPv4-over-IPv6 tunnel) giữa thiết bị của khách hàng (CPE B4) và một bộ định tuyến tại nhà mạng (AFTR), nơi thực hiện NAT44.
- **464XLAT:** Thường được sử dụng trong mạng di động, cho phép các thiết bị IPv6 Only kết nối với dịch vụ IPv4 Only. Nó sử dụng CLAT (Customer Edge Translator) trên thiết bị người dùng để chuyển đổi IPv4 sang IPv6 (NAT46) và PLAT (Provider Edge Translator) tại nhà mạng để chuyển đổi IPv6 sang IPv4 (NAT64).

05

DNS64 và NAT64 hoạt động như thế nào để cho phép thiết bị IPv6 Only truy cập nội dung IPv4?

Khi một thiết bị IPv6 Only muốn truy cập một trang web có địa chỉ IPv4, quá trình diễn ra như sau:

- Thiết bị IPv6 gửi yêu cầu phân giải tên miền (AAAA record) đến máy chủ DNS64.
- Nếu không tìm thấy bản ghi AAAA, DNS64 sẽ truy vấn bản ghi A (IPv4).
- DNS64 nhận địa chỉ IPv4 và tạo ra một bản ghi AAAA tổng hợp bằng cách kết hợp địa chỉ IPv4 (được chuyển đổi sang dạng Hex) với một tiền tố NAT64.
- DNS64 trả về bản ghi AAAA tổng hợp cho thiết bị IPv6.
- Thiết bị IPv6 gửi gói tin đến địa chỉ IPv6 tổng hợp.
- Router NAT64 nhận gói tin IPv6, nhận ra tiền tố NAT64, trích xuất địa chỉ IPv4 đích ban đầu và chuyển đổi địa chỉ IPv6 nguồn của thiết bị thành địa chỉ IPv4 của chính nó (hoặc một địa chỉ được chỉ định).
- NAT64 gửi gói tin IPv4 đến máy chủ đích IPv4.
- Khi nhận được phản hồi IPv4, NAT64 chuyển đổi địa chỉ IPv4 đích thành địa chỉ IPv6 tương ứng (sử dụng tiền tố NAT64) và gửi gói tin IPv6 trở lại thiết bị IPv6 ban đầu.

06

DS-Lite là gì và nó giúp các nhà cung cấp dịch vụ chuyển đổi sang IPv6 Only như thế nào?

DS-Lite (Dual Stack Lite) là một giải pháp giúp các nhà cung cấp dịch vụ (ISP) chuyển đổi sang mạng IPv6 Only trong khi vẫn duy trì khả năng truy cập các dịch vụ IPv4 cho khách hàng. Nó hoạt động bằng cách thiết lập một đường hầm IPv4-over-IPv6 giữa thiết bị của khách hàng (CPE B4) và một bộ định tuyến AFTR (Address Family Transition Router) tại mạng của nhà cung cấp dịch vụ. Tất cả lưu lượng IPv4 từ mạng nội bộ của khách hàng được đóng gói trong các gói tin IPv6 và truyền qua đường hầm đến AFTR. Tại AFTR, các gói tin IPv6 được giải mã để lấy lại gói tin IPv4, sau đó AFTR thực hiện NAT44 để chuyển đổi địa chỉ IPv4 riêng của khách hàng sang địa chỉ IPv4 công cộng trước khi gửi ra Internet IPv4. Phản hồi từ Internet IPv4 được NAT44 trở lại và sau đó được đóng gói lại vào IPv6 để gửi về CPE của khách hàng.

07

Kỹ thuật 464XLAT được sử dụng khi nào và nó khác biệt như thế nào so với DNS64/NAT64?

Kỹ thuật 464XLAT thường được sử dụng trong các trường hợp mà DNS64/NAT64 không hoạt động hiệu quả, ví dụ như khi ứng dụng sử dụng địa chỉ IPv4 trực tiếp (Literal) thay vì tên miền hoặc trong các mạng di động khi điện thoại hoạt động như một điểm phát WiFi chỉ cấp địa chỉ IPv4.

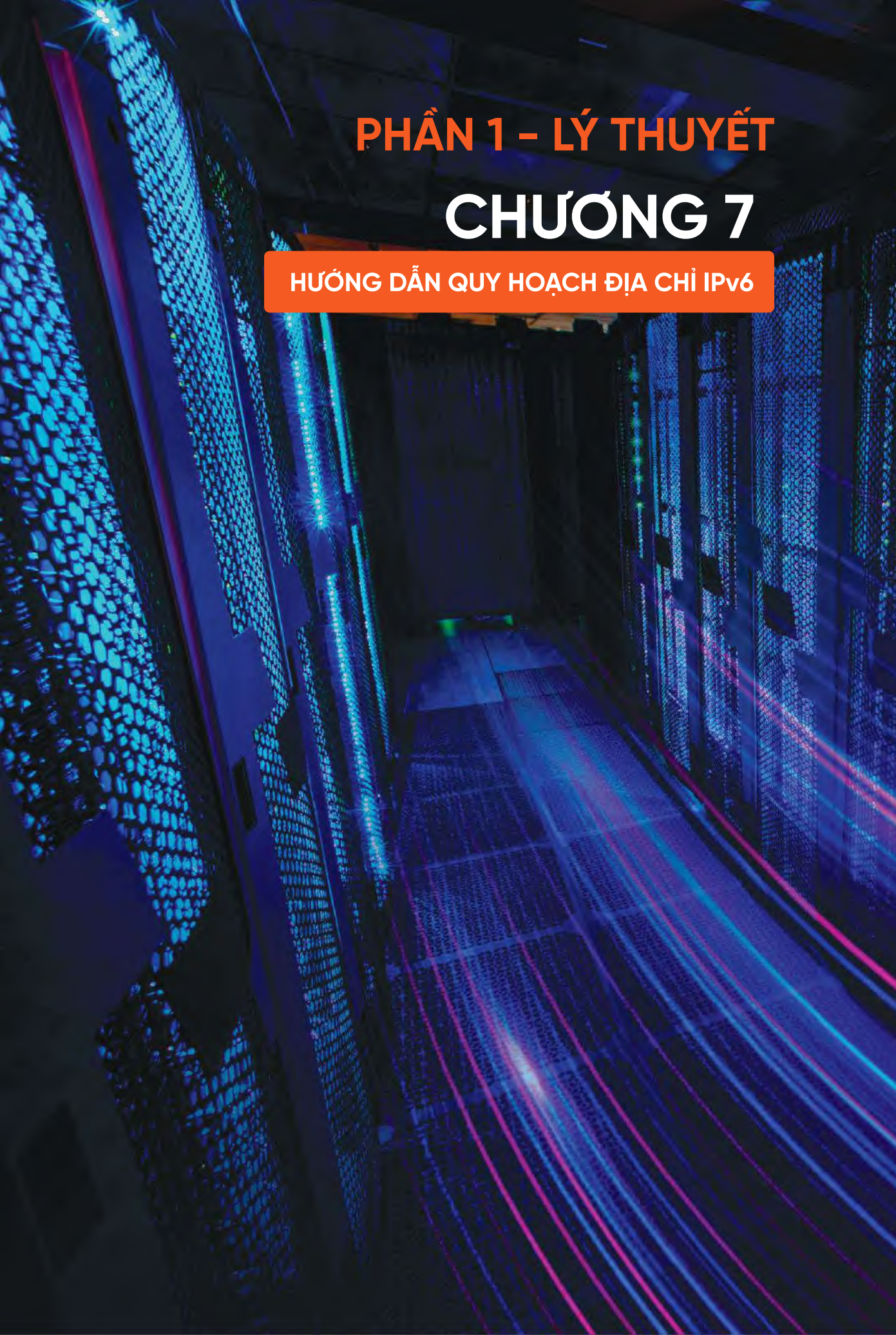
Điểm khác biệt chính là 464XLAT thực hiện chuyển đổi địa chỉ ở cả phía khách hàng (CLAT - NAT46, Stateless, 1:1) và phía nhà mạng (PLAT - NAT64, Stateful, N:1). Trong khi đó, DNS64/NAT64 chủ yếu thực hiện chuyển đổi ở phía mạng (thường là trung tâm dữ liệu hoặc mạng doanh nghiệp). 464XLAT cho phép các thiết bị IPv6 Only kết nối với dịch vụ IPv4 Only một cách hiệu quả hơn trong môi trường mạng di động, giảm sự phụ thuộc vào địa chỉ IPv4 công cộng bằng cách sử dụng địa chỉ IPv4 riêng tại CLAT và chỉ sử dụng IPv4 công cộng tại PLAT khi cần kết nối với dịch vụ IPv4 bên ngoài.

08

IPv6+ là gì và nó mang lại những cải tiến gì so với IPv6 Only?

IPv6+ (hay IPv6-Enhanced) là một khái niệm mới xuất hiện từ năm 2020, được xem là sự mở rộng của IPv6 nhằm đáp ứng các yêu cầu ngày càng cao của hệ thống mạng trong kỷ nguyên 5G, IoT và điện toán đám mây. Trong khi IPv6 tập trung vào việc mở rộng không gian địa chỉ và tối ưu hóa hiệu suất cơ bản, IPv6+ kết hợp với các công nghệ mới để mang lại những cải tiến vượt trội hơn, bao gồm:

- Tối ưu hóa hiệu suất mạng: Giảm độ trễ và tối ưu hóa việc truyền tải dữ liệu thông qua các công nghệ như Segment Routing (SRv6).
- Hỗ trợ cho các công nghệ mạng hiện đại: Tích hợp các công nghệ như Network Slicing để tối ưu hóa phân phối tài nguyên cho các ứng dụng khác nhau, đặc biệt trong mạng 5G.
- Tăng cường khả năng lập trình mạng: Sử dụng các cơ chế như AI-driven Networking để tự động hóa và tối ưu hóa hiệu suất mạng mà không cần sự can thiệp thủ công.
- Tiết kiệm năng lượng và bảo vệ môi trường: Hỗ trợ các giải pháp "mạng xanh" để giảm tiêu thụ năng lượng trong các trung tâm dữ liệu và mạng.
- IPv6+ được xem là bước phát triển tiếp theo của IPv6 Only, hướng tới một hệ thống mạng thông minh hơn, linh hoạt hơn và hiệu quả hơn, đáp ứng tốt hơn các yêu cầu của tương lai. Việc chuyển đổi sang IPv6 Only được coi là tiền đề quan trọng để triển khai các giải pháp IPv6+.



PHẦN 1 – LÝ THUYẾT

CHƯƠNG 7

HƯỚNG DẪN QUY HOẠCH ĐỊA CHỈ IPv6

CHƯƠNG 7

HƯỚNG DẪN QUY HOẠCH ĐỊA CHỈ IPv6

Quy hoạch địa chỉ IPv6 là một bước quan trọng trong kế hoạch chuyển đổi hệ thống mạng sang IPv6. Việc quy hoạch tối ưu không chỉ giúp hệ thống mạng vận hành ổn định mà còn đảm bảo khả năng mở rộng, quản lý dễ dàng và nâng cao hiệu quả định tuyến. Do IPv6 có nhiều khác biệt so với IPv4 nên cách tiếp cận và nguyên tắc quy hoạch cũng thay đổi. Ví dụ, với không gian địa chỉ rộng lớn thì IPv6 không yêu cầu tiết kiệm địa chỉ như IPv4 hoặc việc phân chia Subnet không cần mượn bit từ Interface ID như cơ chế VLSM (Variable Length Subnet Mask) của IPv4. Vì thế khi triển khai IPv6, các tổ chức và doanh nghiệp cần tuân thủ các nguyên tắc quy hoạch của IPv6. Chương này tập trung hướng dẫn cách thức quy hoạch địa chỉ IPv6 cho các tổ chức và doanh nghiệp.

Chương 7 bắt đầu với tầm quan trọng của quy hoạch địa chỉ IPv6, chỉ ra những khác biệt cơ bản so với IPv4. Tiếp đó là các yêu cầu và nguyên tắc chung trong quy hoạch. Trọng tâm của chương là nội dung chi tiết về phân tầng hóa hệ thống mạng, nguyên tắc phân chia subnet, khuyến nghị phân chia theo ranh giới nibble và một số quy định về độ dài prefix. Cuối cùng, tài liệu cung cấp một ví dụ minh họa cụ thể về quy hoạch cho một doanh nghiệp, kèm theo hướng dẫn sử dụng công cụ trực tuyến và cách lưu trữ thông tin sau quy hoạch.

QUA CHƯƠNG NÀY BẠN SẼ NẮM ĐƯỢC:

Tầm quan trọng và các yêu cầu của việc quy hoạch địa chỉ IPv6 trong quá trình chuyển đổi hệ thống mạng.

Những khác biệt cơ bản trong quy hoạch giữa địa chỉ IPv4 và IPv6.

Các nguyên tắc chung quan trọng khi quy hoạch địa chỉ IPv6, bao gồm tính đơn giản, dễ quản lý, khả năng lồng ghép thông tin, dự phòng cho mở rộng và đảm bảo việc gom Route.

Những điều cần chú ý trước khi tiến hành quy hoạch địa chỉ IPv6, như vai trò của Subnet bit, khuyến nghị quy hoạch theo phạm vi 4 bit (Nibble Boundary) và các quy định về độ dài Prefix (Prefix Length) theo các RFC của IETF.

Phương pháp phân tầng hóa hệ thống mạng như một bước đầu tiên trong quy hoạch.

Cách thức **phân chia Subnet theo số bit** và nguyên tắc lồng ghép thông tin về vị trí địa lý và mục đích sử dụng.

Ví dụ **minh họa về quy hoạch** địa chỉ IPv6 cho một doanh nghiệp có trụ sở chính và các chi nhánh.

Hướng dẫn sử dụng **công cụ phân chia Subnet IPv6** trực tuyến và cách kết hợp với phần mềm Excel để lưu trữ và quản lý thông tin quy hoạch địa chỉ một cách hiệu quả.

7.1. YÊU CẦU VÀ NGUYÊN TẮC CHUNG ĐỐI VỚI VIỆC QUY HOẠCH IPv6

7.1.1 Yêu cầu của việc quy hoạch

Do tầm quan trọng của việc quy hoạch địa chỉ IPv6 nên cần đáp ứng các yêu cầu như sau:

Đảm bảo khả năng mở rộng mạng

Các hệ thống mạng luôn cần nâng cấp, mở rộng theo thời gian nên việc quy hoạch cần phải đảm bảo việc mở rộng dễ dàng, không gặp phải giới hạn về địa chỉ IP và tránh tái cấu trúc tốn kém.

Đơn giản hóa quản lý mạng

Một bảng quy hoạch tốt giúp đơn giản hóa việc quản lý mạng và việc giám sát, vận hành và xử lý sự cố cũng dễ dàng hơn.

Hỗ trợ định tuyến hiệu quả

Nếu chúng ta quy hoạch tốt, tuân thủ nguyên tắc gom Route sẽ làm giảm kích thước bảng định tuyến nên việc xử lý định tuyến nhanh hơn và tài nguyên hệ thống được sử dụng tối ưu hơn.

Đảm bảo an toàn và bảo mật

Việc quy hoạch cần phải phân chia các vùng mạng một cách rõ ràng và chi tiết, điều này sẽ giúp cô lập các phạm vi quan trọng và triển khai các cơ chế bảo mật thuận tiện hơn.

7.1.2 Khác biệt giữa quy hoạch địa chỉ IPv4 và IPv6

Có nhiều điểm khác biệt giữa hai giao thức nên điều này ảnh hưởng đến cách thức quy hoạch cho mỗi giao thức. Dưới đây là bảng tổng kết ngắn gọn những điểm khác biệt trong việc quy hoạch cũng như hoạt động của hai giao thức.

Đặc điểm	IPv4	IPv6
Không gian địa chỉ	32 bit (~4.3 tỷ địa chỉ)	128 bit (~340 tỷ tỷ tỷ tỷ địa chỉ)
Yêu cầu quy hoạch	Yêu cầu tiết kiệm địa chỉ, sử dụng NAT	Không đặt nặng vấn đề tiết kiệm mà bảo đảm khả năng mở rộng, không cần sử dụng NAT
Phân bổ địa chỉ	CIDR, VLSM	Thường sử dụng phân chia theo Nibble Boundary (4 bit)
Nguyên tắc phân chia Subnet	Sử dụng các Bit thuộc Host-ID để phân chia mạng con	Phần Interface-ID luôn cố định với 64 bit (trừ 1 số trường hợp đặc biệt), việc phân bổ địa chỉ IPv6 đã bao gồm các bit để phân chia mạng con (nằm trước Interfaec-ID, theo chương 3)
Độ dài Subnet phổ biến	/24, /30, /31, /32	/48, /56, /64
Gom Route (Route Aggregation)	Giới hạn do địa chỉ cạn kiệt	Dễ thực hiện hơn với dải địa chỉ lớn
Khả năng tự cấu hình	Yêu cầu DHCP server	Hỗ trợ SLAAC (Stateless Address Autoconfiguration)

Bảng 9. So sánh một số đặc điểm của IPv4 và IPv6

Trong bảng trên, chúng ta có thể thấy, trong khi IPv4 ưu tiên tìm cách tiết kiệm địa chỉ và sử dụng NAT thì IPv6 hướng đến việc gom Route, hỗ trợ SLAAC, loại bỏ NAT và bảo đảm khả năng mở rộng trong tương lai.

7.1.3 Những nguyên tắc khi quy hoạch địa chỉ IPv6

Quy hoạch địa chỉ IPv6 có một số nguyên tắc chung quan trọng, giúp đảm bảo tính hiệu quả, khả năng mở rộng và dễ quản lý của mạng. Các nguyên tắc này bao gồm:

Đơn giản và dễ quản lý (Simple)

- Việc phân chia tuân theo logic, có cấu trúc rõ ràng, người đọc dễ hiểu và dễ tra cứu thông tin.
- Được lưu trữ dạng bảng hoặc định dạng gần với người dùng như File Excel hoặc Table trong bảng Word hoặc sử dụng phần mềm quản lý địa chỉ chuyên dụng IPAM (IP Address Management).

Lồng ghép thông tin (Embed Information)

- Các Subnet IPv6 nên quy hoạch theo cấu trúc tổ chức của cơ quan, doanh nghiệp, chứa thông tin phản ánh vị trí, vai trò hoặc chức năng của mạng con được phân chia.
- Ví dụ:
  - 2001:db8:1::/48 – Trụ sở chính
  - 2001:db8:2::/48 – Chi nhánh
  - 2001:db8:1:10::/64 – VLAN máy chủ
  - 2001:db8:1:20::/64 – VLAN người dùng
- Điều này giúp việc giám sát, xử lý sự cố và khai báo chính sách bảo mật dễ dàng hơn.

Dự phòng cho mở rộng (Build-in Reserve)

- Việc quy hoạch cần tính đến nhu cầu mở rộng trong tương lai như thêm thiết bị mới, triển khai dịch vụ mới hoặc thay đổi mô hình tổ chức, mở rộng phạm vi địa lý.
- Không phải tất cả các vị trí đều cần dự phòng, cần xem xét và tính toán cho kỹ những vị trí cần thiết để khỏi dự phòng quá mức.

Bảo đảm việc gom Route (Route Aggregation)

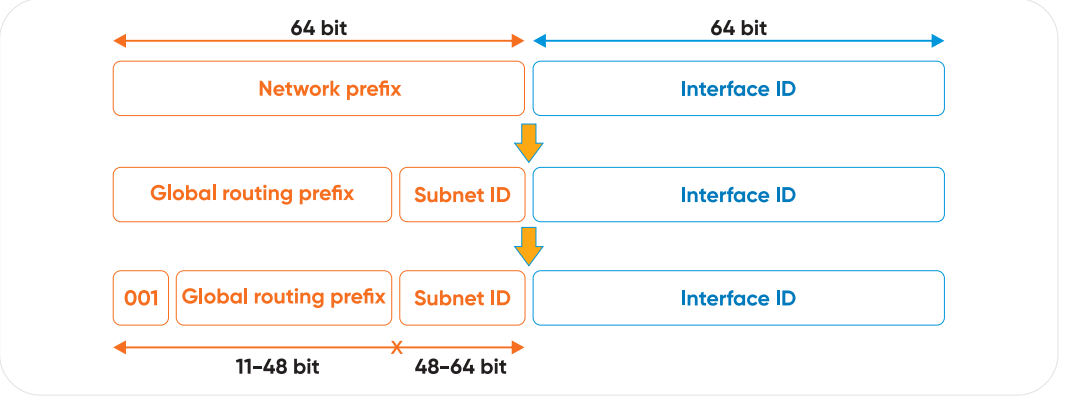
- Sau khi phân bổ và tính toán vị trí dự phòng nên dự phòng Subnet theo chế độ 1+1. Mỗi Subnet được phân bổ sẽ dự phòng thêm một Subnet đúng bằng với Subnet được phân bổ.
- Chế độ dự phòng 1+1 bảo đảm việc mở rộng trong tương lai mà không làm phát sinh thêm Route vì Subnet cũ và mới sẽ được gom thành một. Việc này giúp giảm tải cho router, tăng hiệu suất định tuyến và giúp mạng hoạt động ổn định hơn.

7.2. NHỮNG CHÚ Ý TRƯỚC KHI QUY HOẠCH ĐỊA CHỈ IPv6

Ngoài những yêu cầu và nguyên tắc nêu trên đối với việc quy hoạch địa chỉ IPv6, trong thực tế còn có những quy định (như của IETF) hoặc một số khuyến cáo qua qua thực tiễn triển khai, có một số điều chúng ta cần chú ý. Nội dung dưới đây sẽ nhắc lại một số thông tin về địa chỉ IPv6 và những lưu ý, khuyến cáo trước khi tiến hành quy hoạch.

7.2.1 Subnet bit để quy hoạch IPv6

Như đã giới thiệu trong chương 3 về địa chỉ IPv6 thì phần Interface-ID (tương ứng với phần Host-ID của IPv4) luôn được quy định có độ dài cố định 64 bit. Như vậy các bit dùng để phân chia Subnet sẽ được phân bổ khi cơ quan doanh nghiệp tiến hành đăng ký địa chỉ IPv6. Phần Subnet bit này đứng trước Interface-ID và cùng với Global Routing tạo thành Network Prefix cũng 64 bit.



Hình 98. Vị trí Subnet bit trong địa chỉ IPv6 GUA

Tại Việt Nam, thông thường các cơ quan, doanh nghiệp nếu đăng ký địa chỉ IPv6 qua Trung tâm Internet Việt Nam (VNNIC) thì sẽ được cấp dãy địa chỉ độc lập có độ dài tối thiểu là /48. Với độ dài /48 thì chúng ta còn lại 16 bit phần Subnet nên có thể phân chia đến 2^{16}=65.536 dãy địa chỉ /64. Đây là một số lượng địa chỉ IPv6 rất lớn cho một cơ quan hoặc doanh nghiệp thông thường. Các đơn vị lớn hơn như các nhà mạng thì sẽ đăng ký các dãy lớn ví dụ như /32.

Trong trường hợp đăng ký qua các nhà mạng, thì các cơ quan, doanh nghiệp chỉ có thể đăng ký địa chỉ IPv6 phụ thuộc (PA - Provider Aggregatable) có độ dài có thể là /48, /52/, /56, /60. Tùy theo quy mô của mình các đơn vị có thể đăng ký dãy địa chỉ phù hợp.

Như vậy số bit để phân chia Subnet tùy thuộc vào quy mô thực tế mà cơ quan, doanh nghiệp đăng ký. Với quy mô nhỏ thì việc quy hoạch đơn giản nhưng đối với quy mô lớn thì chúng ta nên cần tính toán kỹ và tuân theo các yêu cầu, nguyên tắc trình bày ở trên.

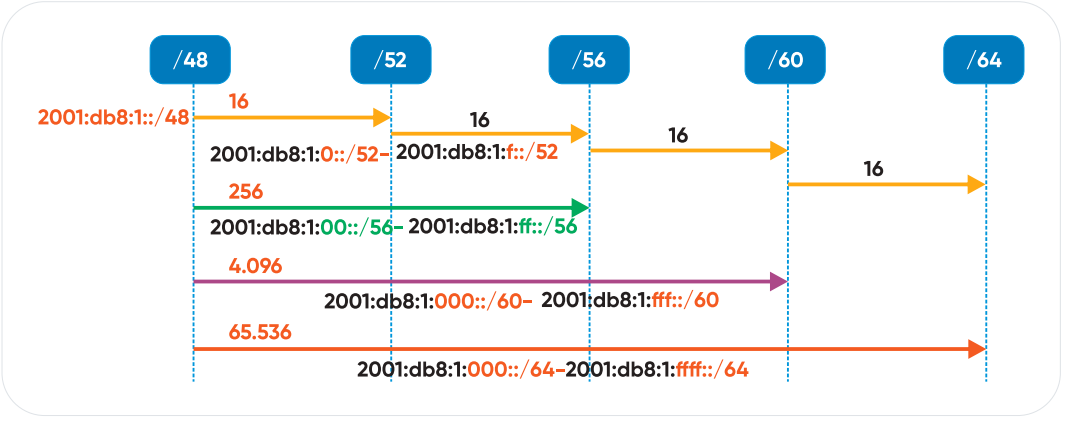
7.2.2 Quy hoạch theo phạm vi 4 bit (Nibble Boundary)

Trước đây đối với IPv4 chúng ta đã quen với khái niệm Octet, đây là tên gọi chỉ một nhóm số có độ dài 8 bit. Địa chỉ IPv6 với độ dài 128 bit được phân ra 16 nhóm (cách nhau bởi dấu :), mỗi nhóm có độ dài 16 bit được gọi Hextet. Ở đây chúng ta làm quen với khái niệm mới là Nibble, dùng để chỉ một nhóm số có độ dài 4 bit. Do địa chỉ IPv6 viết ở dạng Hexa nên mỗi Nibbble tương đương với một chữ số Hexa. Như vậy mỗi Hextet của địa chỉ IPv6 sẽ chứa 4 Nibble.

Ví dụ trong địa chỉ IPv6: 2001:0db8:85a3:0000:0000:8a2e:0370:7334 thì mỗi chữ số trong các cụm như 2001, hoặc 0bd8, 85a3 ... được gọi là Nibble. Khi một Nibble thay đổi thì sẽ tạo ra Subnet khác, ví dụ hai địa chỉ sau thuộc 2 Subnet khác nhau:

- 2001:0db8:85a**3**:0000:0000:8a2e:0370:7334
- 2001:0db8:85a**4**:0000:0000:8a2e:0370:7334

Như vậy, khi chia Subnnet theo Nibble thì chúng ta sẽ có các Prefix là bội số của 4 như: /48, /52, /56. /60. Việc này gúp chúng ta phân biệt các Subnet một cách dễ dàng, trách bị nhầm lẫn trong quy hoạch cũng như quản lý địa chỉ IPv6.



Hình 99. Cách thức phân chia theo Nibble

Dưới đây là ví dụ về việc phân chia địa chỉ theo Nibble và không theo Nibble để chúng ta thấy sự khác biệt.

Prefix /60 (theo Nibble Boundary)

- 2001:db8:0:**0000**::/60 và 2001:db8:0:**0010**::/60 là hai subnet khác nhau.
- Phạm vi địa chỉ của 2001:db8:0:0010::/60: từ 2001:db8:0:**0010**:: đến 2001:db8:0:**001f**::.

```
2001:0db8:0000:0010:0000:0000:0000:0000
                    to
2001:0db8:0000:001f:ffff:ffff:ffff:ffff
```

Hình 100. Ví dụ về phân chia Subnet theo Nibble

Prefix /61 (không theo Nibble Boundary)

- Đây là hai Subnet khác nhau: 2001:db8:0:**0010**::/61 và 2001:db8:0:**0018**::/61, nếu nhìn qua thì chúng ta không thể xác định được chúng cùng hay khác Subnet. Để xác định chúng ta cần chuyển các dãy địa chỉ trên sang dạng nhị phân và đếm số bit tới vị trí 61 và sau đó chuyển ngược lại sang dạng Hexa.

```
2001:0db8:0000:0010:0000:0000:0000:0000
                    to
2001:0db8:0000:0017:ffff:ffff:ffff:ffff
```

Hình 101. Ví dụ về phân chia Subnet không theo Nibble

Như vậy chúng ta có thể thấy việc sử dụng Prefix không theo Nibble sẽ gây khó khăn trong việc quản lý và phân chia địa chỉ. Nên đây là một trong nguyên tắc được khuyến cáo trong việc quy hoạch địa chỉ IPv6. Mặc dù vậy cũng cần cân nhắc việc này vì việc quy hoạch Prefix theo Nibble sẽ làm dư thừa rất nhiều địa chỉ trong nhiều trường hợp. Giả sử một phân vùng mạng nào đó chỉ cần khoảng 8 dãy mạng /64 (giả sử chỉ có tối đa 8 VLAN), tương đương với /61. Nếu chúng ta phân bổ /60 thì số lượng Subnet được phân bổ sẽ dư thừa quá nhiều, gây lãng phí. Như vậy, chúng ta cần tính toán, quy hoạch cân bằng giữa cả tuân theo Nibble và tiết kiệm địa chỉ. Có thể chúng ta sẽ tuân theo Nibble ở một phạm vi nào đó, ở phạm vi nhỏ hơn thì chúng ta sẽ chia nhỏ hơn. Điều này sẽ phù hợp với thực tế hơn.

7.2.3 Một số quy định về IPv6 Prefix Length

Như đã trình bày, địa chỉ IPv6 sẽ gồm hai phần, mỗi phần có độ dài cố định không đổi là 64 bit và không nên sử dụng số bit của Interface ID để phân chia mạng con. Nhưng trong quá trình khai thác các hệ thống IPv6 thực tế, các chuyên gia đã phát hiện một số vấn đề cũng như một số cách hay liên quan đến quy hoạch IPv6 và Prefix Length hợp lý, chính vì thế họ đưa ra các khuyến cáo. IETF đã ban hành các RFC liên quan đến những khuyến cáo này. Sau đây chúng ta điểm qua một số RFC liên quan đến quy định về Prefix Length của IPv6, chúng ta cần phải nắm trước khi thực hiện quy hoạch.

Prefix Length /64 cho thiết bị cuối (RFC 3177)

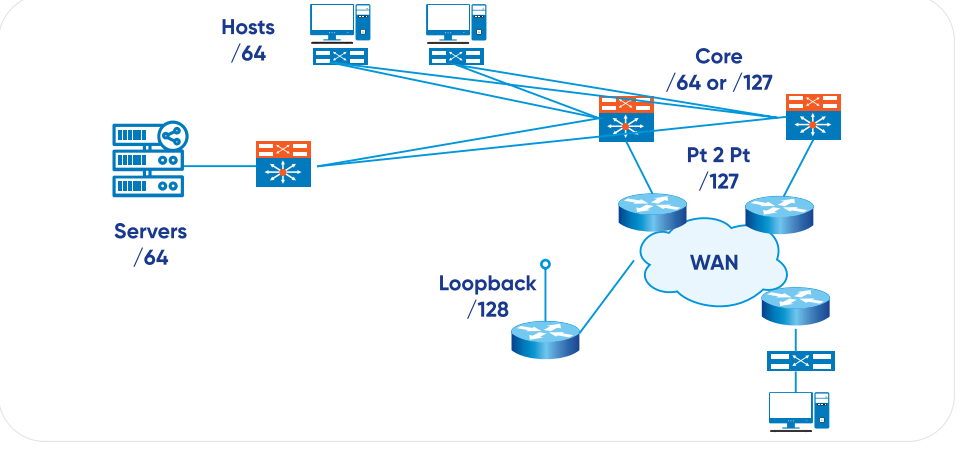
Đối với các thiết bị như máy tính cá nhân, máy chủ hoặc cổng mạng của một thiết bị trên cùng VLAN thì Prefix Length được khuyến nghị sử dụng là /64. Điều này là bắt buộc để các cơ chế như SLAAC và EUI-64 có thể hoạt động. Ngoài ra việc sử dụng Prefix Length /64 đảm bảo số lượng địa chỉ dư thừa cho mỗi VLAN, không cần tính dự phòng trong tương lai cũng như mỗi Host có đủ không gian địa chỉ để hoạt động mà không gặp phải các vấn đề về trùng địa chỉ.

Prefix Length /128 cho cổng Loopback (RFC 3177)

Loopback là một cổng mạng ảo đặc biệt dùng để trao đổi thông tin định tuyến, giám sát và xử lý sự cố. Đối với IPv4, địa chỉ của Interface Loopback có Subnet Mask là 32 bit vì thế RFC 3177 cũng đề xuất sử dụng Prefix /128 cho địa chỉ IPv6. Vì thế chúng ta chỉ cần quy hoạch một dãy địa chỉ /64 dành riêng cho cổng Loopback cho các thiết bị nhưng khi khai báo chỉ sử dụng Prefix /128 cho mỗi cổng Loopback.

Prefix Length /126, /127 cho kết nối Point-to-Point (RFC 6164)

Đối với kết nối Point-to-Point thì thực tế chỉ cần sử dụng hai địa chỉ ở hai đầu. Vì thế với IPv4, chúng ta thường dùng Subnet Mask /30 thậm chí /31 cho kết nối này. Tương tự chúng ta cũng sẽ dùng Prefix /126 hoặc /127 để khai báo IPv6 cho kết nối Point-to-Point. Việc sử dụng Subnet Mask /30 hoặc /31 nhằm tiết kiệm địa chỉ nhưng việc sử dụng Prefix /126 hoặc /127 không phải vì tiết kiệm địa chỉ liên quan đến vấn đề bảo mật. Nếu một người nào đó dùng công cụ để quét (Scan) các địa chỉ thuộc /64 thì giao thức NDP trên thiết bị sẽ tạo ra Neighbor Cache trạng thái INCOMPLETE cho mỗi địa chỉ. Việc này khiến cho bộ nhớ đệm của thiết bị tràn và có thể làm thiết bị ngưng hoạt động. Việc sử dụng /126 hoặc /127 sẽ giúp tránh tình trạng bị tràn này.



Hình 102. Một số Prefix Length đặc biệt

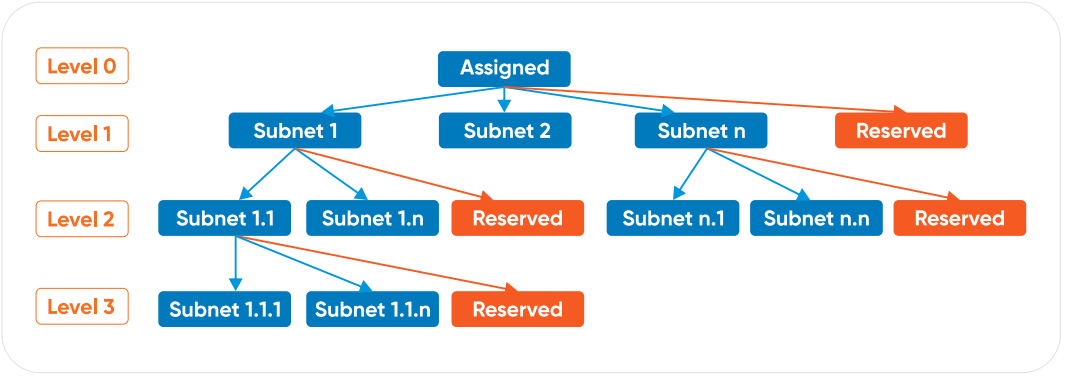
Chúng ta có thể quy hoạch một Subnet /64 dành riêng cho tất cả các kết nối Point to Point trong toàn bộ hệ thống mạng nhưng chỉ phân bổ và khai báo /126 hoặc /127 cho mỗi kết nối. Hoặc chúng ta có thể quy hoạch một /64 cho mỗi kết nối nhưng khi khai báo chỉ sử dụng /126 hoặc /127.

7.3. CÁCH THỨC QUY HOẠCH ĐỊA CHỈ IPv6

Trên đây là những thông tin chung để chuẩn bị cho việc quy hoạch, phần tiếp theo sẽ trình bày các bước thực hiện chi tiết.

7.3.1 Phân tầng hóa hệ thống mạng

Để có cái nhìn trực quan và bảo đảm tính chính xác cho việc quy hoạch thì bước đầu tiên chúng ta cần thực hiện chính là ánh xạ hệ thống mạng cần quy hoạch sang một mô hình phân tầng có cấu trúc.

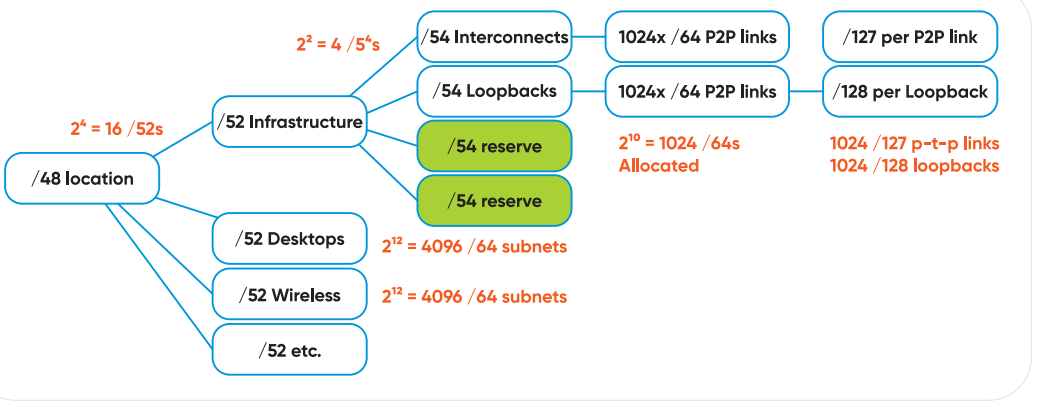


Hình 103. Minh họa việc phân tầng hóa hệ thống

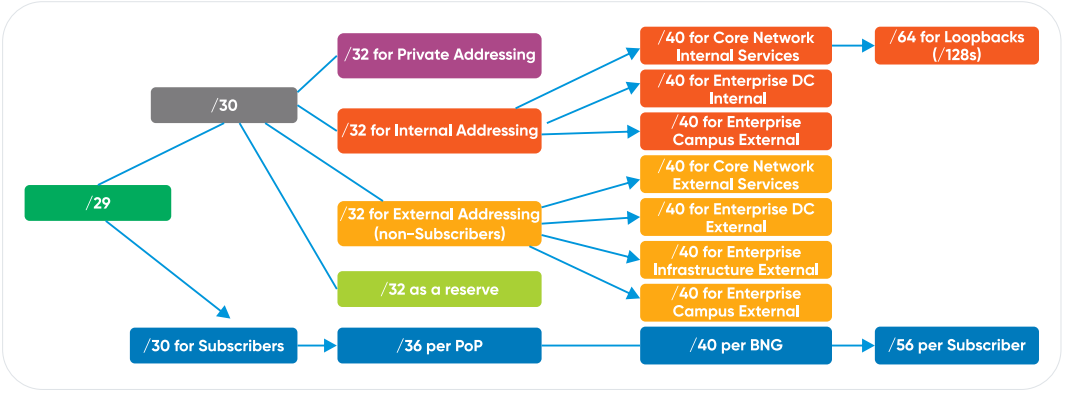
Mô hình này sẽ bắt đầu từ một gốc sau đó phân chia thành các nhánh, các nhánh được phân thành các tầng (Level). Số lượng nhánh và tầng tùy thuộc vào hệ thống thực tế của mỗi cơ quan và doanh nghiệp. Vì thế các bạn cần thống kê hệ thống của mình một cách chính xác để ánh xạ chi tiết hệ thống đó, việc này quyết định rất lớn cho việc quy hoạch. Một điều đáng chú ý là số lượng nhánh tại mỗi tầng không cần phải đều nhau hoặc có những tầng có nhánh con có tầng lại không có nhánh con.

Sau khi sơ đồ hóa hệ thống của mình, chúng ta cần tính toán đến việc dự phòng. Việc dự phòng bắt buộc thực hiện tại các nhánh và các tầng. Số lượng dự phòng được tính theo quy tắc 1+1 hoặc N+1. Việc này tùy thuộc vào quy mô và tính quan trọng của mỗi nhánh. Việc dự phòng 1+1 bảo đảm việc gom Route tối ưu nhưng gây lãng phí địa chỉ. Nếu hệ thống nào thực sự quan trọng và có khả năng mở rộng về sau thì cần tính đến dự phòng 1+1. Với cấu trúc phân tầng và chia nhánh thì tầng trên có khả năng gom Route cho các nhánh trực thuộc bên dưới, bảo đảm mục tiêu gom Route.

Sau khi đã phân tích xong chúng ta cần thực hiện phân bổ Prefix Length theo sơ đồ. Dưới đây là mô hình tham khảo của việc phân tầng cấu trúc mạng và phân bổ Prefix Length.



Hình 104. Ví dụ việc phân tầng IPv6 cho doanh nghiệp



Hình 105. Ví dụ việc phân tầng cho nhà mạng

7.3.2. Phân chia Subnet theo số bit

Như đã trình bày, việc phân chia Subnet trong IPv6 cần tuân thủ dựa trên các nguyên tắc nhằm tối ưu hóa công tác quản lý và vận hành mạng. Một trong những nguyên tắc quan trọng là lồng ghép thông tin (Embed Information), theo đó địa chỉ IPv6 được quy hoạch làm sao chứa thông tin về vị trí, chức năng hoặc mục đích sử dụng của thiết bị hoặc mạng con. Nguyên tắc quan trọng thứ hai là khả năng gom Route (Aggregatable) đóng vai trò quan trọng trong việc tối ưu hóa bảng định tuyến, giảm tải cho các thiết bị router và tăng hiệu suất mạng. Việc kết hợp hai nguyên tắc này tạo giúp việc phân chia Subnet linh hoạt, đáp ứng việc quản lý, vận hành và mở rộng hệ thống mạng về sau.

2001:db8:1234:	L	L	L	L	T	T	T	T	B	B	B	B	B	B	B	B	::/64
2001:db8:1234:	T	T	T	T	B	B	B	B	B	B	B	B	B	B	B	B	::/64

Hình 106. Nguyên tắc phân chia theo số bit từ trái sang phải

Có hai phương pháp lồng ghép thông tin chính: phân chia theo vị trí địa lý (Location) và phân chia theo mục đích sử dụng (Type of use) cho từng nhóm bit. Việc phân chia nhóm bit sẽ được thực hiện từ trái sang phải với mục đích sau:

- **Phân chia theo vị trí (Location):** Các Subnet nằm trong cùng một khu vực địa lý sẽ được gom lại và quảng bá dưới dạng một tuyến đường (Route) duy nhất. Điều này giúp giảm kích thước bảng định tuyến và tăng tốc độ xử lý. Ví dụ, tất cả Subnet trong một tòa nhà hoặc một khu vực cụ thể có thể được gom lại.

- **Phân chia theo mục đích sử dụng (Type of use):** Các Subnet được phân loại theo mục đích sử dụng (ví dụ: phòng kỹ thuật, kinh doanh, máy chủ, người dùng, thiết bị Camera). Điều này giúp dễ dàng áp dụng các chính sách bảo mật (security policy) dựa trên vai trò và chức năng của từng nhóm người dùng, phân vùng mạng hoặc loại thiết bị. Ví dụ, các Subnet dành cho máy chủ sẽ có chính sách bảo mật khác với Subnet dành cho người dùng.

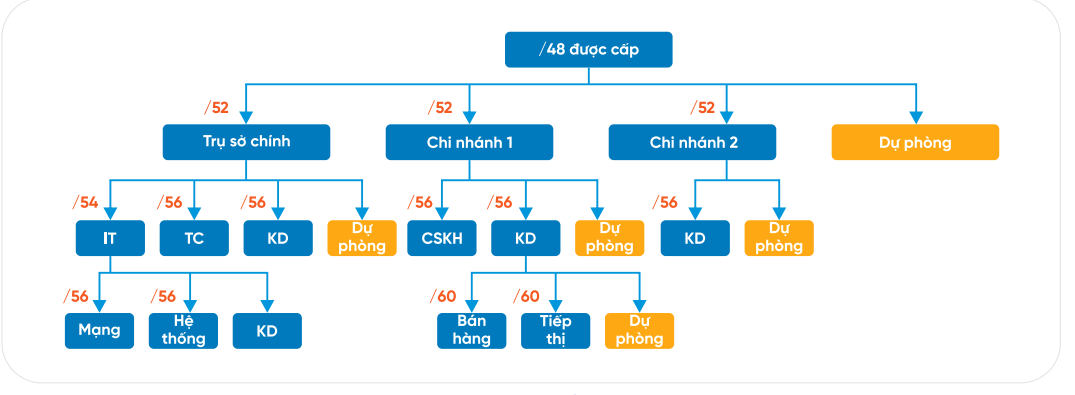
Việc lựa chọn cách phân chia Subnet phụ thuộc vào mục tiêu, mô hình mạng và chính sách bảo mật của từng đơn vị. Một số tổ chức có thể ưu tiên quy hoạch theo vị trí để tối ưu định tuyến, trong khi những đơn vị khác lại tập trung vào mục đích sử dụng để tăng cường bảo mật. Trong nhiều trường hợp, có thể kết hợp cả hai cách một cách hiệu quả: đầu tiên, chia theo vị trí để gom nhóm các Subnet trong cùng khu vực, sau đó tại mỗi vị trí có sử dụng Firewall thì áp dụng phân chia theo mục đích sử dụng để dễ thiết lập Firewall Policy, đảm bảo cả hiệu suất và an ninh mạng đều được duy trì ở mức cao.

Chú ý:
- Chúng ta cần quy hoạch các dãy địa chỉ dành riêng cho kết nối hạ tầng như Point-to-Point, Loopback Interface, Remote VPN ...

7.4. MINH HỌA QUY HOẠCH IPv6 CHO MỘT DOANH NGHIỆP

Trong ví dụ dưới đây, chúng ta xét minh họa quy hoạch của một doanh nghiệp gồm có trụ sở chính và các chi nhánh. Sau khi sơ đồ hóa theo cấu trúc phân tầng, chúng ta bắt đầu phân bổ Prefix Length theo nhu cầu thực tế.

Dưới đây là minh họa cho một doanh nghiệp gồm trụ sở chính và các chi nhánh. Mỗi chi nhánh có các phòng chuyên môn như IT, kinh doanh, tài chính, chăm sóc khách hàng. Tại các phòng ban có các bộ phận hoặc hệ thống nhỏ hơn. Việc mô hình hóa này có thể áp dụng cho doanh nghiệp, cơ quan tổ chức, các trường đại học, các khu công nghiệp, các khách sạn ... Chúng ta phải ánh xạ càng chi tiết thì việc quy hoạch càng chính xác.



Hình 107. Minh họa việc phân tầng và phân bổ Prefix Length cho một doanh nghiệp

Sau khi sơ đồ hóa theo cấu trúc phân tầng, chúng ta bắt đầu tính toán số lượng Subnet để phân bổ Prefix Length phù hợp. Các vị trí cùng cấp có thể được phân bổ số lượng Subnet khác nhau tùy theo nhu cầu thực tế. Việc phân bổ này tuân thủ theo nguyên tắc Nibble và lồng ghép thông tin như đã trình bày. Có thể tại một vị trí nào đó Prefix Length được phân bổ không tuân theo Nibble nhưng đến cấp kế tiếp vẫn tuân theo nguyên tắc Nibble. Việc này thể hiện sự linh hoạt trong quy hoạch địa chỉ IPv6.

Trên đây là quá trình sơ đồ hóa hệ thống mạng cần quy hoạch và tính toán phân bổ Prefix Length cho mỗi vị trí trên sơ đồ. Đây chỉ là bước trực quan hóa hệ thống và cách thức phân bổ địa chỉ. Để phân chia chi tiết và lưu trữ thông tin địa chỉ IPv6 thì chúng ta cần sử dụng ứng dụng Excel hoặc phần mềm chuyên về quản lý địa chỉ IPAM (IP Address Management).

Dưới đây là minh họa việc lưu trữ thông tin quy hoạch địa chỉ IPv6 thông qua phần mềm Excel. Các thông tin trên sơ đồ trên sẽ được ánh xạ vào File Excel như hình sau.

Level 0			Level 1		Level 2	
/48	/50	Phân bổ	/52	**Trụ sở chính**	/54	IT
					/54	Dự phòng IT
					/56	Tài chính
					/56	Kinh doanh
					/55 + /54	Dự phòng chung
			/52	**Chi nhánh 1**	/56	Chăm sóc khách hàng
					/56	Kinh doanh
					/53 + 7*/55	Dự phòng
			/52	**Chi nhánh 2**	/56	Kinh doanh
					/56 + 3*/55 + /53	Dự phòng
			/52	**Dự phòng**		
	/50	**Dự phòng**				
	/49					

Bảng 10. Lưu trữ thông tin quy hoạch bằng Excel

Trong hình này chúng ta cũng phân cấp các Level như trong sơ đồ phân tầng và thực hiện gán Prefix Length. Do đây là cơ sở dữ liệu chúng ta cần ghi chi tiết để những người khác đọc dễ hiểu và chúng ta dễ tra cứu lúc cần như khi quy hoạch thêm hoặc lúc xử lý sự cố, nên cách trình bày có một chút khác biệt trong sơ đồ. Một số giải thích thêm trong File Excel trên:

- Do chúng ta tính toán và phân bổ /52 cho Level 1 nên chúng ta cần phân chia /48 thành nhóm nhỏ hơn gồm /49 và 2*/50. Từ /50 chúng ta phân tách thành 4*/52 và tiến hành phân bổ cho Level 1.
- Tại trụ sở chính, do bộ phận IT quản lý nhiều hệ thống và nhiều thiết bị nên sẽ được phân bổ /54 và được dự phòng theo mô hình 1+1, còn các phòng ban khác được dự phòng chung. Như vậy /52 đầu tiên sẽ phân thành: /52 = /53 + /53 = 2*/54 + 2*/54 = 2*/54 + (2*/55 + /54) = 2*/54 + (2*/56 + /55 + /54).
- Tại chi nhánh 1, do phân bổ bắt đầu /56 nên chúng ta sẽ phân /52 thành: /52 = 2*/53 = 4*/55 + /53 = 2*/56 + 3*/55 + /53.
- Thực hiện tương tự cho chi nhánh 2.

Với cách làm này chúng ta sẽ dễ dàng gom Route cũng như lồng ghép thông tin theo số bit, đồng thời cũng dễ dàng mở rộng, quy hoạch thêm trong tương lai.

Chú ý:
- Chúng ta nên tính cơ chế dự phòng 1+1 hoặc N+1 cho mỗi vị trí và phân bổ dự phòng cho vị trí đó trong File dữ liệu trên.

Đây là bước ánh xạ từ sơ đồ phân tầng sang cơ sở dữ liệu quy hoạch địa chỉ, chúng ta chưa có Prefix đại diện cụ thể tại mỗi Level, mỗi vị trí. Chúng ta cần tiến hành thực hiện phân chia từ dãy địa chỉ /48 được phân bổ. Việc phân chia thủ công khá phức tạp và khả năng sai sót rất dễ xảy ra, vì thế chúng ta cần sử dụng công cụ hỗ trợ phân chia Subnet cho IPv6, giống như các công cụ hỗ trợ cho IPv4 trước đây.

7.5. HƯỚNG DẪN SỬ DỤNG CÔNG CỤ PHÂN CHIA SUBNET IPv6

Hiện nay có rất nhiều công cụ hỗ trợ phân chia Subnet cho IPv6, đặc biệt là ứng dụng trực tuyến, không yêu cầu cài đặt, không cần đăng ký và có thể sử dụng ở bất kỳ nơi nào. Một trong những công cụ phổ biến và hiệu quả là IPv6 Subnet Calculator của Site24x7. Còn có nhiều công cụ khác trên Internet, sau khi làm chủ công cụ này thì các bạn có thể dễ dàng sử dụng các công cụ khác. Để sử dụng công cụ này, các bạn truy cập địa chỉ https://www.site24x7.com/tools/ipv6-subnetcalculator.html. Hoặc các bạn truy cập trang https://www.site24x7.com/, chọn Free Tools, Sysadmin Tools và IPv6 Subnet Conculator.

Dưới đây là cách sử dụng công cụ này:

1. Nhập địa chỉ mạng cần chia (Network Address Block):

Chúng ta nhập địa chỉ mạng gốc muốn phân chia thành các Subnet, trong ví dụ minh họa là 2001:a:b::/48.

Có thể nhập Prefix Length bất kỳ để chia chứ không nhất thiết là /48, ví dụ như nhập vào /52 để tính toán phân chia thành các Subnet /56.

2. Nhập số lượng Subnet cần chia (Number of Subnets):

Tại ô này chúng ta sẽ nhập số lượng các Subnet mà bạn muốn tạo từ địa chỉ mạng gốc đã nhập ở bước trên.

Ví dụ: Nếu muốn chia địa chỉ mạng thành 16 subnet, thì chúng ta lựa chọn "/52 (16 subnets)" trong ô này. Điều này có nghĩa là chúng ta sẽ chia một Network /48 ban đầu thành các Subnet /52.

3. Kết quả phân chia (Subnet Details):

Sau khi chúng ta nhập các thông số, công cụ sẽ tự động hiển thị kết quả phân chia Subnet ngay bên dưới, bao gồm các thông tin:

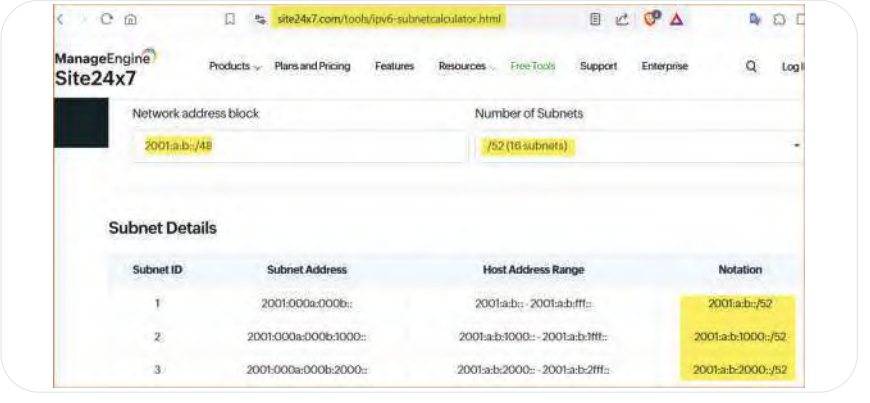
- Subnet ID: Số thứ tự của Subnet.
- Subnet Address: Địa chỉ mạng đại diện của mỗi Subnet.
- Host Address Range: Dải địa chỉ host có thể sử dụng cho mỗi subnet.
- Notation: Dạng biểu diễn rút gọn cho Subnet (ví dụ: "2001:a:b::/52").

4. Ví Dụ:

Nếu chúng ta nhập "2001:a:b::/48" và chọn tạo 16 subnet (/52) thì công cụ cho ra dãy Subnet từ "2001:a:b::/52" đến "2001:a:b:f000::/52".

Chú ý:

- Điểm hay của công cụ này so với các công cụ khác là ở phần Notation, địa chỉ của Subnet được viết gọn theo nguyên tắc rút gọn của địa chỉ IPv6. Việc này giúp dễ đọc, ít sai sót trong ghi chú và giúp việc quản lý địa chỉ IPv6 thuận tiện hơn.



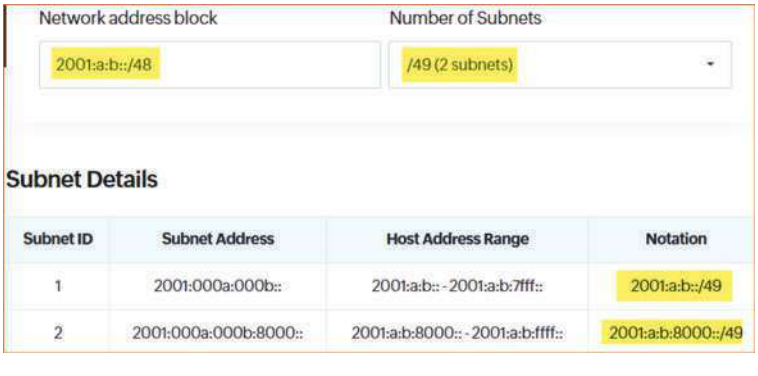
Hình 108. Giao diện của công cụ phân chia địa chỉ IPv6 trực tuyến

7.6. KẾT HỢP CÔNG CỤ CHIA SUBNET VÀ FILE EXCEL

Với mô hình phân tầng, chúng ta đã ánh xạ sang File Excel nhưng thông tin vẫn chưa chi tiết, bằng cách kết hợp với công cụ chia Subnet ở trên, chúng ta tạo dữ liệu quy hoạch địa chỉ IPv6 như sau.

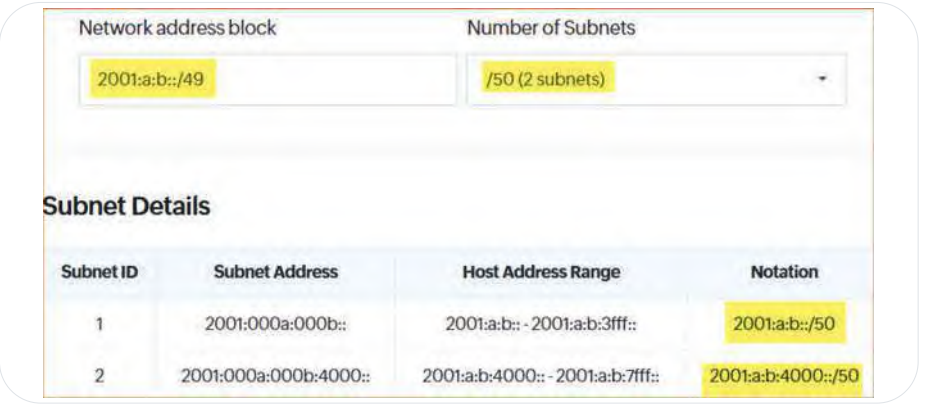
Bước 1:

Tách /48 ban đầu thành 2*/49, trong đó Subnet /49 đầu tiên dùng để phân chia tiếp tục, Subnet /49 còn lại để dự phòng như File Excel.



Hình 109. Thực hiện phân chia Network ban đầu thành Subnet nhỏ hơn

Tách Subnet /49 đầu thành hai /50, trong đó /50 thứ hai để dự phòng.



Hình 110. Thực hiện tương tự cho các Subnet ở Level thấp hơn

Điền các thông tin chi tiết ở trên vào File Excel.

Level 0		
/48	2001:a:b::/50	Phân bổ
	2001:a:b:4000::/50	Dự phòng
	2001:a:b:8000::/49	

Bảng 11. Điền thông tin vào Excel

Bước 2:

- Thực hiện các bước tương tự như bước 1 cho các Level khác.
- Điền toàn bộ và hoàn chỉnh File Excel.

Level 0			Level 1		Level 2	
/48	2001:a:b::/50	Phân bổ	2001:a:b::/52	Trụ sở chính	2001:a:b::/54	IT
					2001:a:b:400::/54	Dự phòng IT
					2001:a:b:800::/56	Tài chính
					2001:a:b:900::/56	Kinh doanh
					2001:a:b:a00::/55 2001:a:b:c00::/54	Dự phòng chung
			2001:a:b:1000::/52	Chi nhánh 1	2001:a:b:1000::/56	Chăm sóc KH
					2001:a:b:1100::/56	Kinh doanh
					2001:a:b:1200::/55 2001:a:b:1400::/55 2001:a:b:1600::/55 2001:a:b:1800::/53	Dự phòng
			2001:a:b:2000::/52	Chi nhánh 2	2001:a:b:2000::/56	Kinh doanh
					2001:a:b:2100::/56 2001:a:b:2200::/55 2001:a:b:2400::/54 2001:a:b:2800::/53	Dự phòng
			2001:a:b:3000::/52	Dự phòng		
	2001:a:b:4000::/50	Dự phòng				
	2001:a:b:8000::/49					

Bảng 12. Chi tiết quy hoạch và phân bổ địa chỉ IPv6 cho các Level trung gian

Bước 3:

- Tiếp tục thực hiện với Level 3. Tùy theo quy hoạch thực tế của mỗi đơn vị chúng ta sẽ phân bổ Prefix Length tương ứng.
- Trường hợp chưa phân bổ chúng ta cũng cần ghi rõ các Subnet dự phòng, để sau này phân bổ tiện hơn.

Level 2		Level 3	
2001:a:b:1100::/56	Kinh doanh	2001:a:b:1100::/64	Nghiên cứu thị trường
		2001:a:b:1101::/64	Bán hàng
		2001:a:b:1102::/64	Marketing
		2001:a:b:1103::/64	Phát triển sản phẩm
		2001:a:b:1104::/64	Quan hệ đối tác
		2001:a:b:1105::/64	Dự phòng
		2001:a:b:1106::/63	
		2001:a:b:1104::/62	
		2001:a:b:1108::/61	
		2001:a:b:1110::/60	
		2001:a:b:1120::/59	
		2001:a:b:1140::/58	
		2001:a:b:1180::/57	

Bảng 13. Chi tiết quy hoạch và phân bổ địa chỉ IPv6 cho các Level cuối cùng

Như vậy, từ việc áp dụng các nguyên tắc quy hoạch, tiến hành phân tầng hệ thống cần quy hoạch, kết hợp sử dụng công cụ chia Subnet và Excel, chúng ta có thể tạo ra một bảng quy hoạch IPv6 đầy đủ và chi tiết cho bất kỳ hệ thống nào.

7.7. TỔNG KẾT CHƯƠNG 7

Chương 7 đã cung cấp hướng dẫn khá chi tiết về quy hoạch địa chỉ IPv6, giúp xây dựng hệ thống mạng hiệu quả và tối ưu hơn. Mở đầu chương là các yêu cầu và nguyên tắc chung khi quy hoạch IPv6, đồng thời so sánh những khác biệt giữa quy hoạch địa chỉ IPv4 và IPv6 nhằm giúp bạn đọc hiểu rõ hơn về sự thay đổi trong cách phân bổ địa chỉ. Tiếp theo, chương 7 đề cập đến các nguyên tắc quan trọng và các lưu ý cần thiết khi lập kế hoạch địa chỉ IPv6, bao gồm việc sử dụng Subnet bit, quy hoạch theo phạm vi 4 bit (Nibble Boundary) và các quy định đặc biệt về IPv6 Prefix Length. Đây là những khái niệm quan trọng giúp đảm bảo tính khoa học và hợp lý trong quá trình triển khai.

Chương này cũng đưa ra phương pháp phân tầng hệ thống mạng và phân chia Subnet theo số bit, giúp tối ưu hóa tài nguyên mạng. Bên cạnh lý thuyết, chương còn cung cấp mô hình minh họa quy hoạch IPv6 cho một doanh nghiệp thực tế, kèm theo hướng dẫn sử dụng công cụ phân chia Subnet IPv6 và kết hợp với Excel để hỗ trợ quản lý hiệu quả hơn. Nhìn chung, chương 7 đã hệ thống hóa các kiến thức cần thiết về quy hoạch địa chỉ IPv6, giúp các tổ chức và doanh nghiệp có thể triển khai IPv6 một cách khoa học, linh hoạt và dễ dàng mở rộng trong tương lai.

7.8. CÂU HỎI ÔN TẬP CHƯƠNG 7

01

Tại sao quy hoạch địa chỉ IPv6 lại quan trọng và khác biệt so với IPv4?

Quy hoạch địa chỉ IPv6 là một bước then chốt trong quá trình chuyển đổi mạng sang IPv6. Việc quy hoạch tối ưu đảm bảo hệ thống mạng hoạt động ổn định, dễ dàng mở rộng, quản lý thuận tiện và nâng cao hiệu quả định tuyến. Điểm khác biệt lớn so với IPv4 là không gian địa chỉ IPv6 khổng lồ (~340 tỷ tỷ tỷ tỷ địa chỉ), loại bỏ nhu cầu tiết kiệm địa chỉ và sử dụng NAT. Thay vào đó, IPv6 tập trung vào khả năng mở rộng, hỗ trợ SLAAC, loại bỏ NAT và ưu tiên gom tuyến (Route Aggregation). Việc phân chia subnet trong IPv6 thường dựa trên Nibble Boundary (4 bit) và phần Interface ID luôn cố định 64 bit, khác với IPv4 sử dụng VLSM và mượn bit từ Host ID để chia Subnet.

02

Những yêu cầu và nguyên tắc chung nào cần tuân thủ khi quy hoạch địa chỉ IPv6?

Việc quy hoạch địa chỉ IPv6 cần đáp ứng các yêu cầu chính sau: đảm bảo khả năng mở rộng mạng dễ dàng, đơn giản hóa quản lý mạng, hỗ trợ định tuyến hiệu quả (gom Route) và đảm bảo an toàn, bảo mật bằng cách phân chia vùng mạng rõ ràng. Các nguyên tắc chung bao gồm:

- **Đơn giản và dễ quản lý:** Phân chia logic, có cấu trúc rõ ràng, dễ hiểu và tra cứu, được lưu trữ khoa học (ví dụ: Excel, IPAM).
- **Lồng ghép thông tin:** Các subnet IPv6 nên phản ánh cấu trúc tổ chức, vị trí, vai trò hoặc chức năng của mạng con.
- **Dự phòng cho mở rộng:** Tính toán đến nhu cầu mở rộng trong tương lai và có cơ chế dự phòng subnet phù hợp (ví dụ: 1+1).
- **Bảo đảm việc gom Route:** Quy hoạch cần tạo điều kiện để gom các dải địa chỉ liên tục thành các tuyến lớn hơn, giảm kích thước bảng định tuyến.

03

Phân chia Subnet trong IPv6 được thực hiện như thế nào và tại sao nên tuân theo Nibble Boundary?

Trong IPv6, phần Interface ID luôn có độ dài cố định là 64 bit. Các bit dùng để phân chia subnet nằm ở phần trước Interface ID, tạo thành Network Prefix (cũng 64 bit). Quy hoạch theo Nibble Boundary (phạm vi 4 bit) được khuyến khích vì giúp phân biệt các subnet một cách dễ dàng, tránh nhầm lẫn trong quản lý. Các prefix thường là bội số của 4 (ví dụ: /48, /52, /56, /60). Mặc dù việc này có thể dẫn đến dư thừa địa chỉ trong một số trường hợp, nhưng nó mang lại sự rõ ràng và đơn giản trong quản lý. Cần cân nhắc giữa việc tuân theo Nibble Boundary và tiết kiệm địa chỉ tùy theo quy mô và yêu cầu cụ thể của mạng.

04

Có những quy định nào về độ dài Prefix (Prefix Length) trong IPv6 cần lưu ý?

IETF đã đưa ra một số khuyến cáo về độ dài Prefix cho các mục đích khác nhau:

- **/64 cho thiết bị cuối (RFC 3177):** Bắt buộc để các cơ chế như SLAAC và EUI-64 hoạt động, đồng thời đảm bảo đủ không gian địa chỉ cho mỗi VLAN.
- **/128 cho cổng Loopback (RFC 3177):** Tương tự như IPv4 (/32), mỗi cổng loopback sẽ có một địa chỉ /128 riêng.
- **/126 hoặc /127 cho kết nối Point-to-Point (RFC 6164):** Không nhằm mục đích tiết kiệm địa chỉ mà để tăng cường bảo mật, tránh bị tràn Neighbor Cache do quét địa chỉ.

05

Phương pháp phân tầng hóa hệ thống mạng đóng vai trò gì trong quy hoạch IPv6?

Phân tầng hóa hệ thống mạng là bước đầu tiên và quan trọng để có cái nhìn trực quan và đảm bảo tính chính xác cho việc quy hoạch IPv6. Bằng cách ánh xạ hệ thống mạng thực tế thành một mô hình phân tầng có cấu trúc (gốc, nhánh, tầng), người quản trị có thể dễ dàng xác định các vùng mạng, mối quan hệ giữa chúng và nhu cầu địa chỉ tại mỗi cấp độ. Việc này giúp việc phân bổ Prefix Length trở nên logic và có hệ thống, đồng thời tạo điều kiện thuận lợi cho việc dự phòng và gom tuyến sau này.

06

Nguyên tắc lồng ghép thông tin và gom Route được áp dụng như thế nào khi phân chia Subnet theo số bit?

Khi phân chia Subnet theo số bit từ trái sang phải, nguyên tắc lồng ghép thông tin được thực hiện bằng cách gán ý nghĩa cho từng nhóm bit trong Prefix, chẳng hạn như vị trí địa lý (Location) hoặc mục đích sử dụng (Type of use). Các Subnet nằm trong cùng một vị trí địa lý hoặc có cùng mục đích sử dụng sẽ có phần Prefix chung, giúp việc gom Route (Route Aggregation) trở nên dễ dàng hơn. Việc gom các Prefix con thành một Prefix lớn hơn giúp giảm kích thước bảng định tuyến trên các router và tăng hiệu suất định tuyến.

07

Làm thế nào để kết hợp sử dụng công cụ phân chia Subnet IPv6 và phần mềm bảng tính (ví dụ: Excel) trong quá trình quy hoạch?

Các công cụ phân chia Subnet IPv6 trực tuyến giúp tự động tạo ra các dải Subnet từ một địa chỉ mạng gốc và độ dài Prefix cho trước. Quá trình kết hợp với Excel thường diễn ra theo các bước sau:

- **Phân tầng và tính toán số lượng Subnet cần thiết** cho mỗi cấp độ trong Excel.
- **Sử dụng công cụ phân chia Subnet** để tạo ra các dải địa chỉ cụ thể dựa trên Prefix Length đã xác định trong Excel.
- **Ghi lại thông tin chi tiết** về từng Subnet (Subnet ID, Subnet Address, Host Address Range, Notation) vào Excel, ánh xạ chúng với các vị trí và chức năng tương ứng trong sơ đồ phân tầng.
- **Lặp lại quá trình** này cho các cấp độ Subnet khác nhau, đảm bảo tính nhất quán và dễ quản lý của bảng quy hoạch.

08

Nội dung chính của chương 7 là gì?

Chương 7 cung cấp một hướng dẫn toàn diện về quy hoạch địa chỉ IPv6, bao gồm:

- **Các yêu cầu và nguyên tắc chung** khi quy hoạch, so sánh với IPv4.
- **Các nguyên tắc quan trọng và lưu ý cần thiết**, như sử dụng Subnet bit, quy hoạch theo Nibble Boundary và các quy định về Prefix Length.
- **Phương pháp phân tầng hóa hệ thống mạng** và phân chia Subnet theo số bit để tối ưu hóa tài nguyên.
- **Mô hình minh họa quy hoạch IPv6 cho doanh nghiệp**, bao gồm trụ sở chính và chi nhánh.
- **Hướng dẫn sử dụng công cụ phân chia Subnet IPv6** (ví dụ: Site24x7) và cách kết hợp với Excel để quản lý thông tin quy hoạch một cách hiệu quả.

PHẦN 2 – THỰC HÀNH

CHƯƠNG 8

HƯỚNG DẪN TRIỂN KHAI MÔ HÌNH IPv6 DUAL STACK

Tiếp nối phần lý thuyết về giao thức IPv6 chương này sẽ tập trung vào vấn đề triển khai thực tế IPv6 cho các hệ thống mạng. Đặc biệt, **nội dung được thiết kế dành cho các tổ chức và doanh nghiệp** sở hữu địa chỉ IP/ASN độc lập và kết nối đa hướng nhằm giúp các đơn vị xây dựng một hạ tầng mạng hiện đại, bảo mật và đáp ứng các yêu cầu mở rộng trong tương lai. Chương 8 tập trung hướng dẫn triển khai thực tế giao thức IPv6 theo mô hình Dual Stack, cho phép IPv4 và IPv6 hoạt động đồng thời. Nội dung chi tiết bao gồm các hướng dẫn cấu hình từ cơ bản đến nâng cao, như gán địa chỉ tĩnh, cấp phát động qua SLAAC và DHCPv6, cùng các giao thức định tuyến OSPFv3, iBGP và eBGP, nhằm trang bị kiến thức và kỹ năng cần thiết cho chuyên gia mạng trong việc triển khai IPv6 hiệu quả.

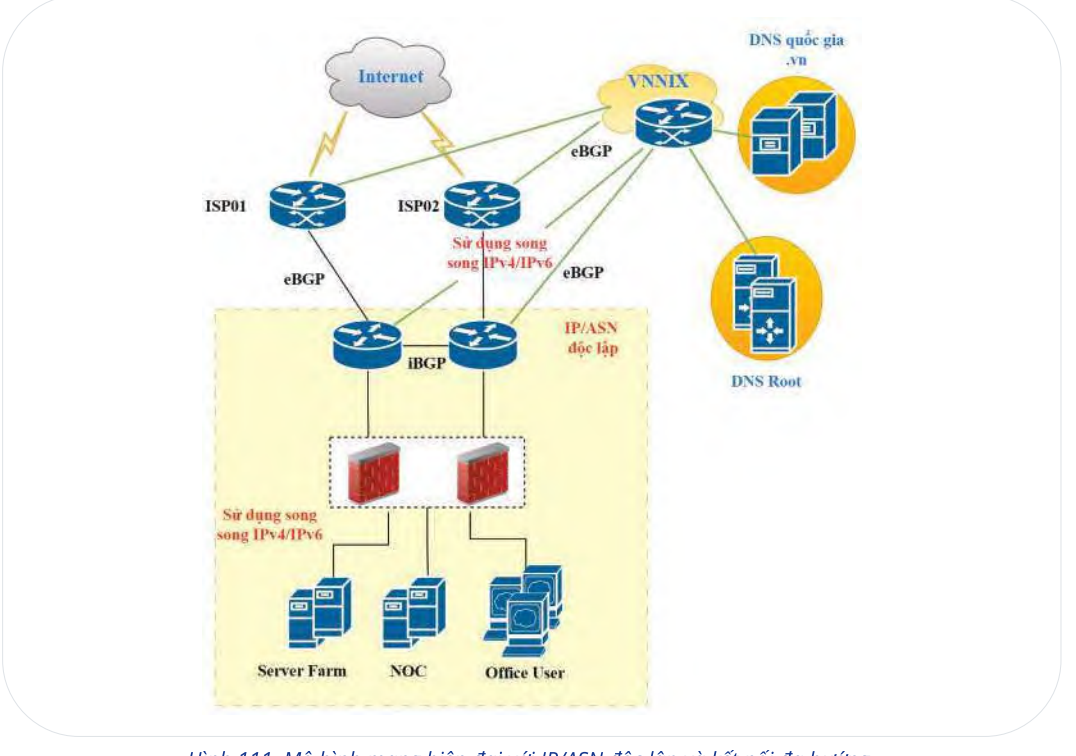
Qua chương này bạn sẽ:

- Hiểu rõ về **lợi ích của việc sở hữu IP/ASN độc lập và kết nối đa hướng (Multi-homing).**
- Nắm cách **cấu hình IPv6** từ cơ bản đến nâng cao, bao gồm: gán địa chỉ IP tĩnh, các kỹ thuật cấp IP động như **SLAAC, DHCPv6, VRRPv3** và các giao thức định tuyến như **OSPF và BGP.**
- Nắm cách cấu hình chi tiết **10 bài LAB thực hành.**
- Làm chủ việc khai báo IPv6 đối với **các giao thức và dịch vụ mạng** quan trọng nhất theo mô hình Dual Stack cho hệ thống mạng của mình.

8.1. MÔ HÌNH MẠNG HIỆN ĐẠI DUAL STACK CHO DOANH NGHIỆP, CƠ QUAN VÀ TỔ CHỨC VỚI IP/ASN ĐỘC LẬP VÀ ĐA HƯỚNG

Trong bối cảnh chuyển đổi số, các doanh nghiệp, tổ chức, cơ quan chính phủ và các trường đại học tại Việt Nam ngày càng đòi hỏi một hệ thống mạng hiện đại, ổn định và an toàn để đảm bảo hoạt động liên tục và hiệu quả. Việc sở hữu địa chỉ địa chỉ IP độc lập (PI) mang lại lợi thế lớn khi cho phép các đơn vị kết nối linh hoạt với nhiều nhà mạng mà không lo gián đoạn dịch vụ, đồng thời tự mình xây dựng, quản lý chính sách bảo mật và định tuyến dữ liệu. Để triển khai địa chỉ IP độc lập, các tổ chức cần đăng ký số hiệu mạng ASN (Autonomous System Number) – định danh hệ thống mạng trên Internet, nhằm hỗ trợ quản lý dãy IP độc lập và quảng bá qua giao thức định tuyến BGP.

Bên cạnh đó, kết nối đa hướng (Multi-homing) là giải pháp thiết yếu cho các doanh nghiệp và cơ quan yêu cầu tính sẵn sàng cao. Bằng cách thiết lập kết nối đồng thời với nhiều ISP, Multi-homing đảm bảo hệ thống tự động chuyển mạch lưu lượng sang các kết nối dự phòng khi một ISP gặp sự cố, duy trì hoạt động không gián đoạn. Hơn nữa, giải pháp này còn tối ưu hóa tốc độ truy cập Internet bằng cách lựa chọn tuyến đường tốt nhất, nâng cao chất lượng dịch vụ cho các tổ chức.



Hình 111. Mô hình mạng hiện đại với IP/ASN độc lập và kết nối đa hướng

Để nâng cao hiệu quả và tính ổn định, các doanh nghiệp và cơ quan có thể triển khai kết nối tới VNIX – nơi tích hợp hệ thống DNS quốc gia và kết nối trực tiếp với DNS Root. Sự kết hợp giữa IP độc lập, Multi-homing, kết nối VNIX và hệ thống DNS tạo nên một mô hình mạng tối ưu, giúp tăng băng thông, cải thiện khả năng dự phòng, nâng cao hiệu suất và bảo đảm tính sẵn sàng.

Vì thế, chương này sẽ bao gồm các bài LAB khai báo nâng cao về triển khai iBGP và eBGP cho mạng doanh nghiệp và tổ chức sử dụng IP/ASN độc lập và kết nối đa hướng.

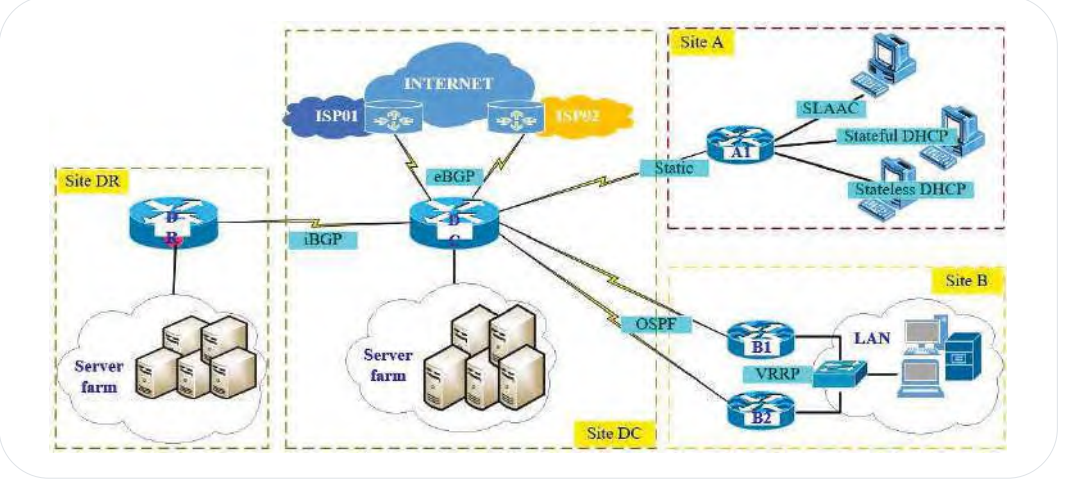
8.2. MÔ HÌNH VÀ NỘI DUNG LAB IPv6 DUAL STACK

Nội dung chính của chương này là thực hành khai báo IPv6 ở chế độ Dual Stack, gồm cả IPv4 và IPv6 hoạt động đồng thời. Các khai báo hiện tại cho IPv4 sẽ được áp dụng cho IPv6, ví dụ như định tuyến tĩnh, OSPF, BGP, VRRP ... Chúng ta đã quen thuộc với khai báo với IPv4 nên những nội dung liên quan đến IPv4 sẽ không được trình bày ở đây mà chỉ tập trung vào khai báo cho IPv6.

Chú ý:

- Nội dung LAB này chỉ dành cho Dual Stack, nếu hệ thống hoạt động ở chế độ IPv6 Only thì cần triển khai thêm DNS64 và NAT64. Nội dung thực hành cho IPv6 Only sẽ được trình bày ở chương tiếp theo. Chương này giúp các bạn làm quen với khai báo IPv6 cho các giao thức và dịch vụ chính yếu của hạ tầng mạng.

Hệ thống mạng trong mô hình LAB này được thiết kế để triển khai giao thức IPv6 với mô hình IP và ASN độc lập, đồng thời tận dụng các giao thức định tuyến khác nhau nhằm đảm bảo tính linh hoạt, hiệu quả và khả năng dự phòng cao. Các thành phần chính của mô hình LAB gồm:



Hình 112. Mô hình LAB tổng thể

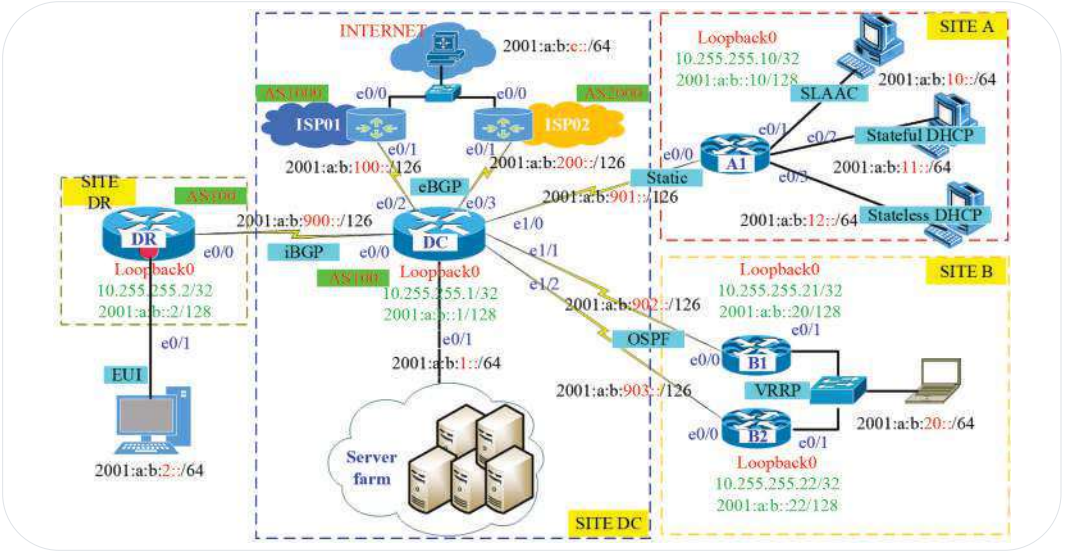
Trung tâm dữ liệu (Site DC): Kết nối với hệ thống dự phòng (Site DR) thông qua giao thức iBGP, đảm bảo trao đổi thông tin định tuyến nội bộ giữa các địa điểm. Đồng thời, DC cũng thiết lập kết nối eBGP Multihoming với các ISP hoặc hệ thống VNIX để đảm bảo khả năng kết nối đa hướng nhằm tối ưu hóa lưu lượng Internet.

Chi nhánh A: Chỉ có một kết nối duy nhất đến Site DC, sử dụng Default Route để cấu hình đơn giản và phù hợp cho các hệ thống nhỏ gọn.

Chi nhánh B: Có hai kết nối đến Site DC nên áp dụng giao thức OSPF nhằm cân bằng tải và dự phòng động trường hợp xảy ra sự cố với một kết nối.

Các mạng LAN: Để cung cấp địa chỉ IPv6 cho máy tính nội bộ thì các kỹ thuật như SLAAC, Stateful và Stateless DHCPv6 được sử dụng để tối ưu hóa việc cấp phát. VRRP cũng được triển khai để cung cấp khả năng dự phòng Default Gateway cho các máy tính nội bộ tại Site B. Toàn bộ kiến trúc này được thiết kế nhằm đảm bảo sự ổn định, tối ưu hóa và tính dự phòng của hệ thống mạng.

Quy hoạch địa chỉ IP và ASN: Site DC và Site DR sẽ sử dụng AS 100, các ISP01 và ISP02 sử dụng lần lượt AS 100 và AS 200. Về địa chỉ Loopback, địa chỉ đấu nối cũng như tên của từng cổng được thể hiện ở hình bên dưới. Địa chỉ Loopback IPv4 được sử dụng làm Router ID cho các router vì không thể sử dụng IPv6 làm Router ID.



Hình 113. Chi tiết thông tin quy hoạch cho bài LAB

Chú ý:

- Các thiết bị mạng được sử dụng trong bài LAB là của của hãng Cisco, sử dụng hệ điều hành IOS. Điều này giúp đơn giản hóa việc trình bày và bạn đọc cũng dễ tìm hiểu thêm thông tin vì các các tài liệu về thiết bị Cisco có khá nhiều trên mạng Internet.
- Các giao thức được sử dụng là OSPF, BGP và VRRP là giao thức chuẩn cho thiết bị của tất cả các hãng.
- Bài LAB được giả lập trên môi trường của phần mềm EVE-NG Community.
- Địa chỉ 2001:a:b::/48 chỉ là địa chỉ minh họa cho các bài LAB giúp nội dung trình bày gọn gàng hơn, trong thực tế cần sử dụng địa chỉ được phân bổ cho tổ chức, doanh nghiệp.

8.3. CÁC BÀI LAB CHI TIẾT CHO MÔ HÌNH DUAL STACK

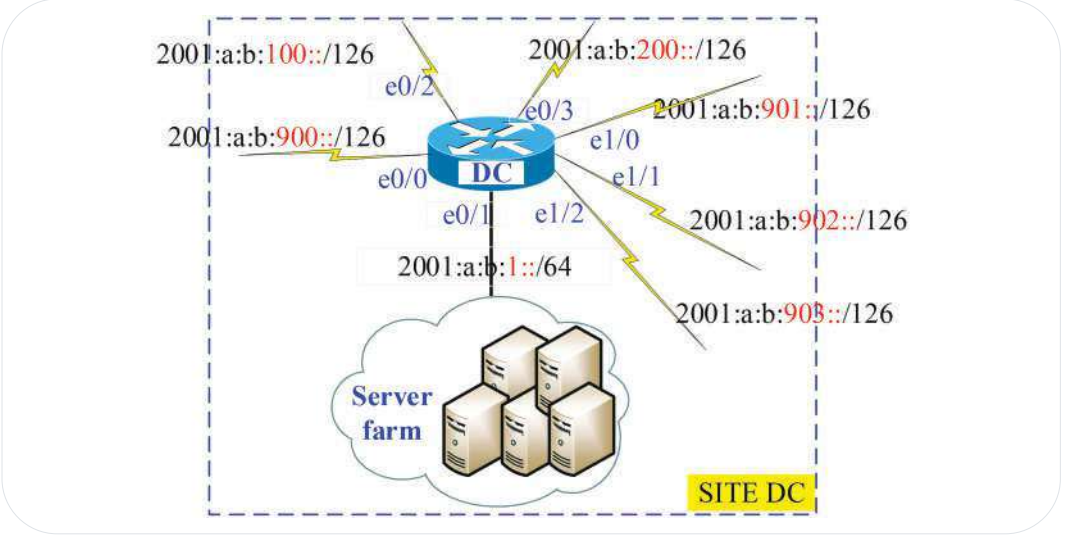
Nội dung thực hành của chương này bao gồm 10 bài LAB chi tiết, được thiết kế để cung cấp các khai báo cơ bản và phổ biến nhất, phù hợp cho hệ thống mạng của doanh nghiệp cũng như các trung tâm dữ liệu trong môi trường Dual Stack. Các bài LAB bắt đầu từ việc cấu hình địa chỉ IPv6 tĩnh trên router và các hệ điều hành như Windows cùng Ubuntu, sau đó mở rộng sang các phương pháp gán địa chỉ động thông qua SLAAC, Stateful DHCPv6 và Stateless DHCPv6. Ngoài ra, chương này còn hướng dẫn cấu hình giao thức dự phòng VRRPv3 để tăng cường độ tin cậy, cùng với các kỹ thuật định tuyến như Static Route, giao thức định tuyến OSPFv3, iBGP và eBGP. Qua đó, các bạn sẽ nắm vững các kỹ năng cơ bản và nâng cao để triển khai và quản lý hiệu quả mạng Dual Stack trong các tình huống thực tế.

Bài LAB	Nội dung
LAB01	Cấu hình địa chỉ IPv6 tĩnh cho router
LAB02	Cấu hình địa chỉ IPv6 tĩnh cho Windows và Ubuntu
LAB03	Cấu hình địa chỉ IPv6 động bằng SLAAC
LAB04	Cấu hình địa chỉ IPv6 động bằng Stateful DHCPv6
LAB05	Cấu hình địa chỉ IPv6 động bằng Stateless DHCPv6
LAB06	Cấu hình giao thức dự phòng VRRPv3
LAB07	Cấu hình định tuyến tĩnh (Static Route)
LAB08	Cấu hình giao thức định tuyến OSPFv3
LAB09	Cấu hình giao thức định tuyến iBGP
LAB10	Cấu hình giao thức định tuyến eBGP

Bảng 14. Các bài LAB chi tiết cho mạng Dual Stack

8.4. LAB01 - CẤU HÌNH ĐỊA CHỈ IPv6 TĨNH CHO ROUTER

Trong các hệ thống mạng có rất nhiều thiết bị cần gán địa chỉ IP tĩnh như các máy chủ, các thiết bị mạng router, Firewall, các Camera và thậm chí cả các máy tính cá nhân. Dưới đây là minh họa về khai báo địa chỉ IPv6 tĩnh cho thiết bị Router DC.



Hình 114. Chi tiết quy hoạch và phân bổ địa chỉ IPv6 cho các Level

```
!
ipv6 unicast-routing
!
interface Ethernet0/0
 description To_Router_DR
 ipv6 address 2001:A:B:900::1/126
!
```

Đây là cấu hình địa chỉ IPv6 tĩnh cho cổng Ethernet0/0 trên Route-DC. Các cổng khác của router này được khai báo tương tự. Cần phải khai báo lệnh "ipv6 unicast-routing" nhằm bật chế độ định tuyến cho giao thức IPv6, lúc này việc định tuyến tĩnh và động mới có thể hoạt động.

Trong sơ đồ LAB trên, địa chỉ trên các cổng của Router đều là :1.

Sau khi khai báo địa chỉ IPv6 tĩnh, chúng ta kiểm tra các thông tin khai báo như sau:

```
Router_DC#show ipv6 interface brief
Ethernet0/0            [up/up]
    FE80::A8BB:CCFF:FE00:2000   Địa chỉ Link local
    2001:A:B:900::1             Địa chỉ Global Unicast
```

Trong hình trên, dù chúng ta chỉ khai báo địa chỉ Global Unicast tĩnh nhưng địa chỉ Link Local được tự động sinh ra. Link Local là địa chỉ bắt buộc phải có, có thể được cấu hình thủ công và mỗi Interface chỉ có duy nhất một địa chỉ Link Local, trong khi có thể gán nhiều địa chỉ Global Unicast cho một Interface.

Lệnh phía dưới hiển thị địa chỉ MAC của Interface e0/1, chú ý kỹ chúng ta sẽ thấy 64 bit cuối địa chỉ Link Local ở trên gần giống với địa chỉ MAC. Điều này là do địa chỉ Link Local được sinh ra từ địa chỉ MAC theo cấu trúc EUI-64 như đã giới thiệu.

```
Router_DC#show interfaces e0/1
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.2000 (bia aabb.cc00.2000)
  Description: To_Router_DR
```

Địa chỉ MAC

Ngoài ra chúng ta có thể cấu hình địa chỉ IPv6 tĩnh cho các Interface theo cấu trúc EUI-64 như sau, đây là ví dụ khai báo trên cổng Ethernet0/2 của Router_DR:

```
interface Ethernet0/1
 description To_LAN
 no ip address
 ipv6 address 2001:A:B:2::/64 eui-64
 ipv6 enable!
```

Chỉ khai prefix

Kiểm tra kết quả sau khai báo cho thấy địa chỉ Global Unicast và Link Local đều có 64 bit Interface ID giống nhau vì đều cùng sử dụng cấu trúc EUI-64.

```
Router_DR#show ipv6 interface e0/1
Ethernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is
FE80::A8BB:CCFF:FE00:1010
Description: To_LAN
  Global unicast address(es):
    2001:A:B:2:A8BB:CCFF:FE00:1010, subnet is
2001:A:B:2::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1010
```

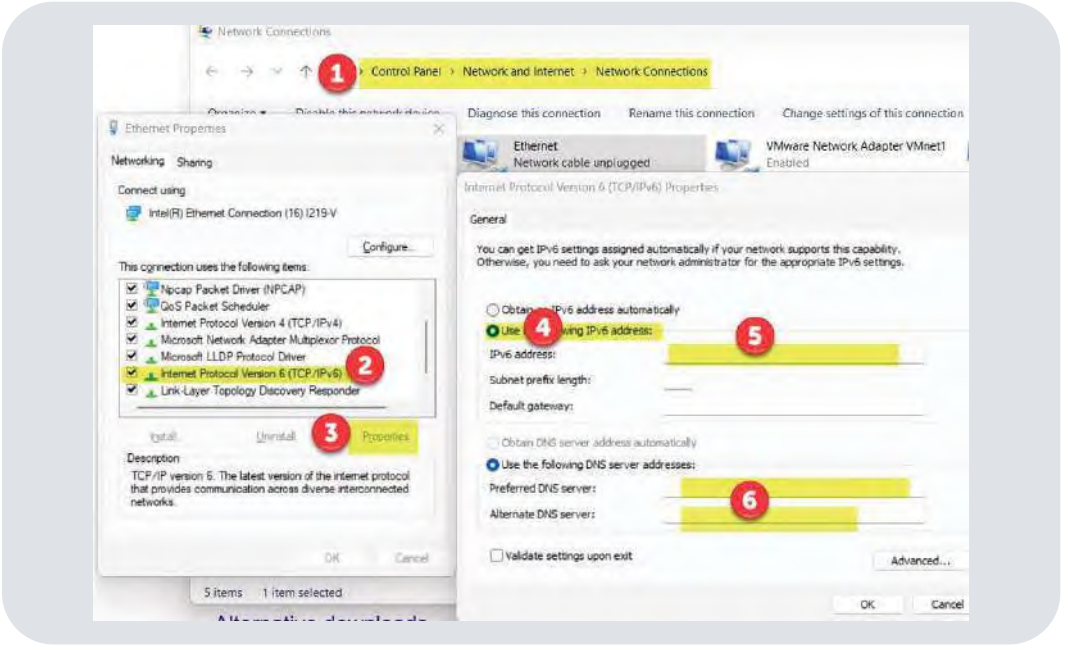
8.5. LAB02 - CẤU HÌNH ĐỊA CHỈ IPv6 TĨNH CHO WINDOWS VÀ UBUNTU

Hiện nay các hệ điều hành máy tính đã hỗ trợ IPv6 nên việc khai báo địa chỉ IPv6 rất đơn giản, dưới đây là khai báo địa chỉ IPv6 tĩnh cho Windows và Unbuntu.

8.5.1. Khai báo IPv6 cho Windows

Mặc định hệ điều hành Windows đã bật sẵn giao thức IPv6 và hoạt động ở chế độ nhận địa chỉ IPv6 tự động. Việc nhận IPv6 động có thể từ DHCPv6 hoặc theo cơ chế SLAAC. Dưới đây là cách thức chuyển từ chế độ nhận địa chỉ IPv6 động sang khai báo tĩnh:

- Vào **Control Pannel** → **Network and Internet** → **Network Connections**
- Nhấp phải vào **Card mạng** cần gán IPv6 tĩnh, chọn **Properties** → Chọn giao thức **IPv6** → **Properties**
- Chọn **Use the following IPv6 address** và điền vào địa chỉ IPv6 cần gán → điền địa chỉ IPv6 của **DNS Server**.



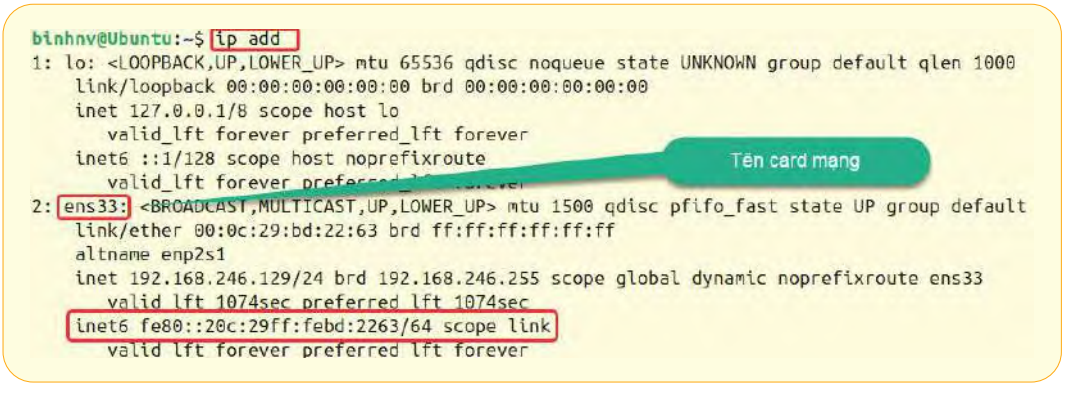
Hình 115. Hướng dẫn khai báo IPv6 cho Windows

Chú ý: Địa chỉ IPv6 của một số DNS Server phổ biến trên thế giới:

Đơn vị	IPv4	IPv6
Google	8.8.8.8	2001:4860:4860::8888
	8.8.4.4	2001:4860:4860::8844
OpenDNS	208.67.222.222	2620:119:35::35
	208.67.220.220	2620:119:53::53
Cloudflare	1.1.1.1	2606:4700:4700::1111
	1.0.0.1	2606:4700:4700::1001

8.5.2. Khai báo IPv6 cho Ubuntu

Cũng như Windows, các hệ điều hành Ubuntu cũng đã hỗ trợ IPv6 mặc định. Để khai báo địa chỉ IPv6 tĩnh cho Ubuntu thì đầu tiên cần kiểm tra tên Card mạng cần gán địa chỉ bằng lệnh **"ip address"**. Sau đó xác định tên của Card mạng như hình dưới.



Hình 116. Kiểm tra tên Card mạng

Tiếp theo thực hiện gán địa chỉ IPv6 cho Card mạng ở trên bằng dòng lệnh như bên dưới và thực hiện kiểm tra địa chỉ IPv6 đã gán.

Để khai báo địa chỉ IPv6 tĩnh cho các phiên bản Ubuntu từ 17.04 trở đi thì chúng ta cần dùng công cụ "netplan", công cụ này sẽ thay đổi có File cấu hình mạng có đuôi là **".yaml"** trong thư mục **"/etc/netplan/"** vì thế cần kiểm tra tên File này trước.

```
binhnv@Ubuntu:~$ ll /etc/netplan/
tổng 20
drwxr-xr-x   2 root root  4096 Jan  2 11:11 ./
drwxr-xr-x 139 root root 12288 Jan  2 11:17 ../
-rw-------   1 root root   390 Jan  2 10:17 50-cloud-init.yaml
```

Hình 117. Kiểm tra tên của File cấu hình của Netplan

Tiếp theo sử dụng **"netplan"** để bắt đầu sửa chữa File cấu hình ở trên:

```
binhnv@Ubuntu:~$ sudo nano /etc/netplan/50-cloud-init.yaml
```

Hình 118. Lệnh để sửa File cấu hình Netplan

Lúc này xuất hiện cửa sổ cho phép thay đổi các thông tin liên quan đến địa chỉ IPv4, IPv6, khai báo DNS, Default Gateway. Hình dưới là mô tả khai báo đồng thời cả địa chỉ IPv4 và IPv6 tĩnh.

```
 GNU nano 7.2                          /etc/netplan/50-cloud-init.yaml
# This file is generated from information provided by the datasource.  Changes
# to it will not persist across an instance reboot.  To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
    ethernets:
        ens33:
            dhcp4: false
            addresses: [192.168.100.2/24]
            addresses: [2001:a:b:1::2/64]
            gateway4: 192.168.100.1
            gateway6: 2001:a:b:1::1
            nameservers:
               addresses: [8.8.8.8, 8.8.4.4]
               addresses: [2001:4860:4860::8888, 2001:4860:4860::8844]
    version: 2
```

Hình 119. Thay đổi thông tin tương ứng với quy hoạch của bài LAB

Sau đó thực hiện áp dụng các cấu hình đã khai báo bằng lệnh sau:

```
binhnv@Ubuntu:~$ sudo netplan apply

** (generate:3750): WARNING **: 14:27:20.891: `gateway4` has been depre
ad.
See the 'Default routes' section of the documentation for more details.

** (generate:3750): WARNING **: 14:27:20.892: `gateway6` has been depre
ad.
See the 'Default routes' section of the documentation for more details.
```

Hình 120. Áp dụng khai báo mới cho Netplan

Tiếp theo kiểm tra những thông số đã khai báo, kết quả địa chỉ IPv4 và IPv6 đã thay đổi.

```
binhnv@Ubuntu:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 10
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group defaul
    link/ether 00:0c:29:bd:22:63 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.100.2/24 brd 192.168.100.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 2001:a:b:1::2/64 scope global noprefixroute
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:febd:2263/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Hình 121. Kiểm tra kết quả sau khai báo

Kiểm tra địa chỉ Default Gateway:

```
binhnv@Ubuntu:~$ ip route
default via 192.168.100.1 dev ens33 proto static metric 20100
192.168.100.0/24 dev ens33 proto kernel scope link src 192.168.100.2 metric 100
binhnv@Ubuntu:~$
binhnv@Ubuntu:~$ ip -6 route
2001:a:b:1::/64 dev ens33 proto kernel metric 100 pref medium
fe80::/64 dev ens33 proto kernel metric 1024 pref medium
default via 2001:a:b:1::1 dev ens33 proto static metric 20100 pref medium
```

Hình 122. Kiểm tra IPv6 Gateway

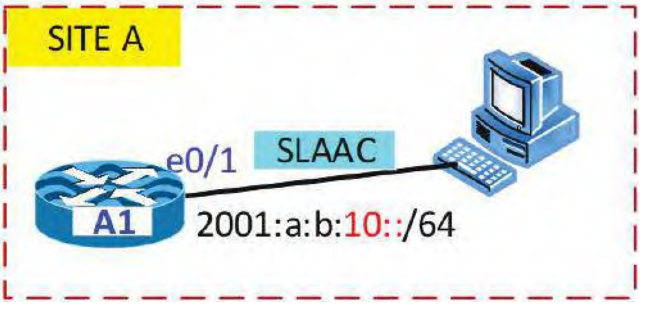
Hoặc có thể dùng lệnh **"nmcli dev show <tên_giao_diện> | grep DNS"** để xem tất cả các thông tin liên quan đã khai báo:

```
binhnv@Ubuntu:~$ nmcli dev show ens33
GENERAL.DEVICE:                         ens33
GENERAL.TYPE:                           ethernet
GENERAL.HWADDR:                         00:0C:29:BD:22:63
GENERAL.MTU:                            1500
GENERAL.STATE:                          100 (đã kết nối)
GENERAL.CONNECTION:                     netplan-ens33
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/ActiveConnectio
WIRED-PROPERTIES.CARRIER:               bật
IP4.ADDRESS[1]:                         192.168.100.2/24
IP4.GATEWAY:                            192.168.100.1
IP4.ROUTE[1]:                           dst = 0.0.0.0/0, nh = 192.168.100.1, mt = 20100
IP4.ROUTE[2]:                           dst = 192.168.100.0/24, nh = 0.0.0.0, mt = 100
IP4.DNS[1]:                             8.8.8.8
IP4.DNS[2]:                             8.8.4.4
IP6.ADDRESS[1]:                         fe80::20c:29ff:febd:2263/64
IP6.ADDRESS[2]:                         2001:a:b:1::2/64
IP6.GATEWAY:                            2001:a:b:1::1
IP6.ROUTE[1]:                           dst = 2001:a:b:1::/64, nh = ::, mt = 100
IP6.ROUTE[2]:                           dst = ::/0, nh = 2001:a:b:1::1, mt = 20100
IP6.ROUTE[3]:                           dst = fe80::/64, nh = ::, mt = 1024
IP6.DNS[1]:                             2001:4860:4860::8888
IP6.DNS[2]:                             2001:4860:4860::8844
```

Hình 123. Kiểm tra đầy đủ các thông tin về địa chỉ IPv4, IPv6.

8.6. LAB03 – CẤU HÌNH ĐỊA CHỈ IPv6 ĐỘNG BẰNG SLAAC

Kỹ thuật SLAAC (Stateless Address Autoconfiguration) cho phép các thiết bị tự động cấu hình địa chỉ IPv6 mà không cần dùng đến DHCP Server. Đây là một trong những tính năng nổi bật của IPv6 giúp giảm thiểu sự phức tạp trong việc quản lý địa chỉ IP, phù hợp với các hệ thống mạng lớn, đặc biệt là trong lĩnh vực IoT. Hầu hết các hệ điều hành hiện đại như Linux, Windows, macOS, FreeBSD, Android và iOS cũng như các thiết bị mạng đều hỗ trợ IPv6 SLAAC.



Hình 124. Mô hình của bài LAB về SLAAC

Dưới đây là khai báo địa chỉ cho cổng Ethernet 0/0 trên Router Site_A:

```
Router_A1#show running-config | begin 0/1
interface Ethernet0/1
 description To_LAN_SLAAC
 no ip address
 ipv6 address 2001:A:B:10::1/64
 ipv6 enable
```

Kiểm tra chi tiết chúng ta thấy cổng Ethernet 0/1 đã tự động bật chế độ SLAAC (Stateless Autoconfig).

```
Router_A1#show ipv6 interface e0/1
Ethernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is
FE80::A8BB:CCFF:FE00:7010
  Description: To_LAN_SLAAC
  Global unicast address(es):
    2001:A:B:10::1, subnet is 2001:A:B:10::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF00:7010
  Hosts use stateless autoconfig for addresses.
```

Mặc định, các interface của Router đều bật chế độ stateless autoconfig

Các thiết bị trong mạng có thể tự động khai báo địa chỉ IPv6 cho mình bằng cách sau:

- Thiết bị gửi bản tin RS (Router Solicitation) đến các router.
- Sau đó router phản hồi bằng bản tin RA (Router Advertisement) chứa Prefix /64.
- Thiết bị nhận được Prefix sẽ kết hợp với địa chỉ Interface ID tự tạo bằng EUI-64 hoặc ngẫu nhiên để thành địa chỉ IPv6 duy nhất trên mạng.
- Tiếp theo thiết bị sẽ áp dụng kỹ thuật kiểm trùng DAD (Duplicate Address Detection) trước khi địa chỉ IPv6 tự tạo có thể được sử dụng.

Hình dưới đây là địa chỉ của một máy tính sử dụng SLAAC với cấu trúc EUI-64.

```
LINK-LOCAL SCOPE       : fe80::250:79ff:fe66:680b/64
GLOBAL SCOPE           : 2001:a:b:10:2050:79ff:fe66:680b/64
DNS                    :
MAC                    : 00:50:79:66:68:0b
```

Tự tạo địa chỉ dựa theo Prefix của Router + EUI-64

SLAAC chỉ cho phép tạo địa chỉ IPv6 một cách tự động chứ không thể cung cấp thông tin về DNS Server, điều này làm hạn chế kết nối thông qua tên miền (Domain Name). Chính vì thế RFC 6106 đã đưa ra quy định cho phép các router có thể quảng bá thông tin DNS trong bản tin Router Advertisement. Dưới đây là cấu hình DNS bổ sung cho kỹ thuật SLAAC. Chính vì thế khi đầu tư thiết bị router cần yêu cầu hỗ trợ RFC 6106.

SLAAC mặc dù cho phép các thiết bị tự động tạo địa chỉ IPv6 nhưng có một hạn chế là không cung cấp thông tin về máy chủ DNS, gây khó khăn cho việc truy cập các tài nguyên mạng thông qua tên miền (Domain Name). Để khắc phục, RFC 6106 đã được ban hành, cho phép các router quảng bá thông tin DNS trong các bản tin RA (Router Advertisement). Nhờ đó, các thiết bị có thể tự động cấu hình địa chỉ IPv6, đồng thời có cả thông tin về DNS Server, đảm bảo khả năng kết nối đầy đủ. Do vậy, khi lựa chọn thiết bị router cho mạng IPv6, cần yêu cầu hỗ trợ RFC 6106 để đảm bảo hoạt động cho thiết bị.

```
Router_A1#show running-config | begin 0/1
interface Ethernet0/1
 description To_LAN_SLAAC
 ipv6 address 2001:A:B:10::1/64
 ipv6 enable
 ipv6 nd ra dns server 2001:4860:4860::8888
```

8.7. LAB04 – CẤU HÌNH ĐỊA CHỈ IPv6 ĐỘNG BẰNG STATEFULL DHCPV6

Thông thường, DHCP Server ngoài cung cấp địa chỉ và các thông tin khác như địa chỉ DNS Server, tên miền nội bộ thì DHCP Server cần quản lý địa chỉ IP được cấp cho máy tính nào, thời gian cấp (Leased-time) bao lâu ... Chính khả năng lưu trữ và quản lý trạng thái (State) của địa chỉ IP đã cấp nên tên gọi đầy đủ của Server này là Stateful DHCPv6 Server.

DHCP Server có thể được khai báo trên máy chủ Windows, Linux, Router và Firewall. Dưới đây là minh họa khai báo DHCP Server trên thiết bị router của Cisco. Trong cấu hình này router thông qua bản tin RA (Router Advertisement) thông báo cho máy trạm sử dụng DHCP Server để cấp phát địa chỉ. Điều này được thể hiện qua lệnh **"managed-config-flag".**

```
!
Router_A1#show running-config | begin dhcp
ipv6 dhcp pool stateful_pool
 address prefix 2001:A:B:11::/64
 dns-server 2001:A:B:1::53
 domain-name vnnic.lab
!
Router_A1#show running-config | begin 0/2
interface Ethernet0/2
 description To_LAN_Stateful
 no ip address
 ipv6 address 2001:A:B:11::1/64
 ipv6 enable
 ipv6 nd managed-config-flag
 ipv6 dhcp server statefull_pool
!
```

Yêu cầu client nhận IP từ DHCP

Đây là thông tin mà máy trạm nhận được, hoàn toàn đúng theo cấu hình từ DHCP Server.

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix . ..: vnnic.lab
   IPv6 Address. . . . . . . . . . . : 2001:a:b:11:8495:6872:1771:4e17
   IPv6 Address. . . . . . . . . . . .: 2001:a:b:11:b0a4:bfd2:2cdc:7143
   Temporary IPv6 Address. . . . . .: 2001:a:b:11:ad55:5c4c:a018:4cb8
   Link-local IPv6 Address. . . . . : fe80::8495:6872:1771:4e17%11
   IPv4 Address. . . . . . . . . . . : 10.1.1.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . ..: fe80::a8bb:ccff:fe00:120%11
                                         10.1.1.1
```

Hình 125. Kiểm tra địa chỉ IPv6 Client nhận được

Thông tin trạng thái (State) trên DHCP Server được thể hiện rõ như sau:

```
Router_A1#show ipv6 dhcp binding
Client: FE80::8495:6872:1771:4E17
  DUID: 000100011C840564525400123456
  Username : unassigned
  VRF : default
  IA NA: IA ID 0x0E525400, T1 43200, T2 69120
    Address: 2001:A:B:11:B0A4:BFD2:2CDC:7143
            preferred lifetime 86400, valid lifetime 172800
            expires at Jan 11 2025 10:55 AM (169818 seconds)
```

```
Có một số lệnh khác để kiểm tra thông tin chi tiết của DHCP Server như:
show ipv6 dhcp pool
show ipv6 dhcp interface
```

8.8. LAB05 - CẤU HÌNH ĐỊA CHỈ IPv6 ĐỘNG BẰNG STATELESS DHCPV6

Stateless DHCPv6, tính năng chỉ có ở giao thức IPv6, là sự kết hợp hoạt động của SLAAC và DHCP truyền thống. SLAAC có nhiệm vụ hỗ trợ tạo IPv6 tự động như đã trình bày ở phần trước còn DHCP thì cung cấp các thông tin khác như DNS, Domain Name. Stateless không cung cấp địa chỉ IPv6, nên không cần lưu trữ thông tin đã cấp.

Stateless DHCPv6 là một giải pháp hiệu quả và linh hoạt trong việc cấp địa chỉ IPv6 động, đặc biệt là cho các mạng lớn và phức tạp. Giải pháp giúp đơn giản hóa việc quản lý địa chỉ IP, giảm tải cho máy chủ DHCP, tăng khả năng mở rộng và tận dụng đặc tính của SLAAC. Dù vậy giải pháp này cũng có một số hạn chế so với Stateful DHCP, ví dụ nó không hỗ trợ cấp phát Prefix Delegation (PD).

Prefix Delegation (PD cho phép một router (thường là của khách hàng, ví dụ Modem FTTH) nhận nhiều dãy địa chỉ IPv6 (Prefix) từ một router khác (thường là router của nhà mạng). Như vậy ngoài nhận địa chỉ IPv6 cho cổng WAN thì Modem khách hàng còn nhận thêm một dãy địa chỉ IPv6 để cấp cho các thiết bị mạng bên trong (như Wifi Client).

Dưới đây là cấu hình minh họa cho Stateless DHCPv6 trên Router Cisco. Trong thực tế có thể có thể sử dụng kết hợp tính năng SLAAC trên Router với DHCP Server trên các hệ thống khác.

```
!
 Router_A1#show running-config | begin stateless
ipv6 dhcp pool stateless_pool
 dns-server 2001:A:B:1::53    Không cần khai báo IPv6 prefix
 domain-name vnnic.lab
!
Router_A1#show running-config | begin 0/3
interface Ethernet0/3
 no ip address
 ipv6 address 2001:A:B:12::1/64
 ipv6 nd other-config-flag
 ipv6 dhcp server stateless_pool
!
```

Khác với Stateful DHCPv6 thì IPv6 Pool ở đây không khai báo IPv6 Prefix mà chỉ khai báo các thông tin cung cấp thêm cho máy trạm. Một thông tin quan trọng ở đây là router gửi bản tin RA có chứa cụm từ "nd other-config-flag" nhằm thông báo cho máy trạm tự gán địa chỉ IPv6 và liên hệ DHCP Server để nhận thêm các thông tin khác.

8.9. LAB06 - CẤU HÌNH GIAO THỨC DỰ PHÒNG VRRPV3

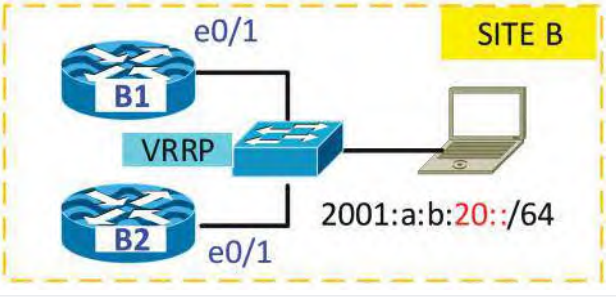
VRRP (Virtual Router Redundancy Protocol) là giao thức dự phòng, cho phép nhiều router hoạt động như một router ảo nhằm tăng tính sẵn sàng cho hệ thống mạng. Đối với IPv6, cần dùng VRRPv3 vì phiên bản này hỗ trợ cả IPv4 và IPv6. Để cấu hình VRRP cho IPv6 thì cần phải có hai thông tin chính:

Địa chỉ Link-Local ảo

Các router và thiết bị trong cùng phân đoạn mạng thường dùng địa chỉ IPv6 Link-local dùng để trao đổi với nhau. Đối với VRRPv3 bắt buộc phải có địa chỉ Link-local ảo để các thiết bị khác chọn làm Default Gateway nên nó được khai báo trước tiên.

Địa chỉ Unicast ảo

Đây là địa chỉ ảo tương ứng với địa chỉ Unicast của mỗi router tham gia VRRPv3, tương tự như đối với VRRPv2. Các thiết bị trong mạng có thể khai báo tĩnh dùng địa chỉ này làm Default Gateway.



Hình 126. Mô hình của bài LAB về VRRPv3

Dưới đây là cấu hình cho VRRP, trình tự khai báo như sau:

- Kích hoạt VRRPv3 trên router.
- Cấu hình địa chỉ Link-Local ảo.
- Cấu hình địa chỉ Unicast ảo.
- Điều chỉnh các thông số VRRP khác như priority (ưu tiên) và timers (thời gian kiểm tra trạng thái) nếu cần.
- Khai báo Track để chuyển trạng thái khi một kết nối nào đó bị sự cố.

Dưới đây là khai báo chi tiết cho 2 router B1 và B2 trong sơ đồ trên. Cổng Ethernet0/0 là cổng Uplink của hai router nên cần giám sát (Track) cổng để chuyển trạng thái của VRRP nếu cổng Ethernet0/0 bị sự cố.

```
Router_B1#show running-config
fhrp version vrrp v3
!
track 1 interface Ethernet0/0 line-protocol
!
interface Ethernet0/1
 description To_LAN
 ipv6 address 2001:A:B:20::2/64
 ipv6 enable
 vrrp 1 address-family ipv6
  priority 110
  track 1 decrement 50
  address FE80::12:1 primary    Địa chỉ virtual
  address 2001:A:B:20::1/64
  exit-vrrp
```

```
Router_B2#show running-config
fhrp version vrrp v3
!
track 1 interface Ethernet0/0 line-protocol
!
interface Ethernet0/1
 description To_LAN
 ipv6 address 2001:A:B:20::3/64
 ipv6 enable
 vrrp 1 address-family ipv6
  track 1 decrement 50
  address FE80::12:1 primary
  address 2001:A:B:20::1/64    Địa chỉ virtual
  exit-vrrp
```

Sau khi khai báo cho VRRP, dùng các lệnh sau để kiểm tra trạng thái và thông tin của VRRP.

```
Router_B1#show vrrp brief
 Interface Grp A-F Pri Time Own Pre State Master addr/Group addr
 Et0/1     1   IPv6 110  0   N   Y  MASTER  FE80::A8BB:CCFF:FE00:510(local) FE80::12:1
```

```
Router_B1#show vrrp ipv6
Ethernet0/1 - Group 1 - Address-Family IPv6
  State is MASTER
  State duration 2 days 18 hours 17 mins
  Virtual IP address is FE80::12:1
  Virtual secondary IP addresses:
    2001:A: B:20::1/64
  Virtual MAC address is 0000.5E00.0201
  Advertisement interval is 1000 msec
  Preemption enabled
  Priority is 110
    Track object 1 state UNDEFINED decrement 50
  Master Router is FE80::A8BB:CCFF:FE00:510 (local), priority is 110
  Master Advertisement interval is 1000 msec (expires in 146 msec)
  Master Down interval is unknown
```

```
Router_B2#show ipv6 interface e0/1
Ethernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is
FE80::A8BB:CCFF:FE00:9010 [UNA]
Virtual link-local address(es):   Địa chỉ virtual
    FE80::12:1 [UNA/OOD]
  Description: To_LAN
  Global unicast address(es):
    2001:A:B:20::1, subnet is 2001:A:B:20::/64 [UNA/OOD/VIRT]
    2001:A:B:20::3, subnet is 2001:A:B:20::/64
  Joined group address(es):
    FF02::1
FF02::2
    FF02::12        Địa chỉ multicast để VRRP trao đổi bản tin
    FF02::1:FF00:3
    FF02::1:FF00:9010
```

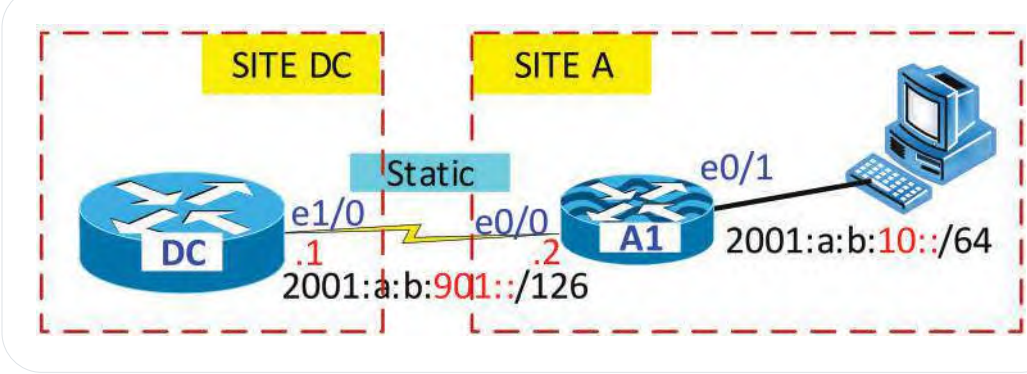
Trong trường hợp khai báo VRRP thì kỹ thuật SLAAC vẫn hoạt động bình thường, các máy trạm vẫn có thể tự gán địa chỉ IPv6 động.

```
C:\Users\inant>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : lan
   IPv6 Address. . . . . . . . . . . : fd00:db80::3700:f6e9:efd4:4e05
   Temporary IPv6 Address. . . . . . : fd00:db80::db9:9522:8b7b:f198
   Temporary IPv6 Address. . . . . . : fd00:db80::6c82:9474:3964:be5a
   Temporary IPv6 Address. . . . . . : fd00:db80::896e:4740:9059:3025
   Temporary IPv6 Address. . . . . . : fd00:db80::dc26:bee0:d91:30d9
   Link-local IPv6 Address . . . . . : fe80::6c27:608b:777b:c44b%6
   IPv4 Address. . . . . . . . . . . : 192.168.100.30
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.100.1
```

Hình 127. SLAAC vẫn hoạt động tốt với VRRPv3

8.10. LAB07 – CẤU HÌNH ĐỊNH TUYẾN TĨNH (STATIC ROUTE)

Trong minh họa này, Site_A chỉ có một kết nối ra bên ngoài với Site_DC nên ở đây chúng ta sử dụng định tuyến tĩnh. Từ Router Site_DC sẽ khai Static Route về Site_A trong khi Router Site_A trỏ Default Route sang Site-DC.



Hình 128. Mô hình của bài LAB về Static Route

```
!
Router_DC#show running-config | begin route
ipv6 route 2001:A:B:10::/64 2001:A:B:901::2
!
```

```
!
Router_A1#show running-config | begin route
ipv6 route ::/0 2001:A:B:901::1
!  Router_A1 khai Default Route!
```

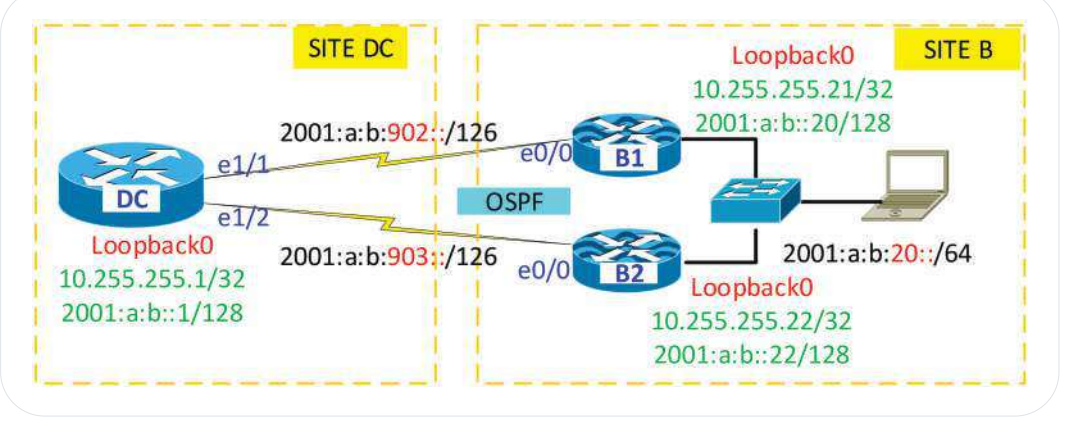
Kiểm tra thông tin định tuyến và kết nối sau khai báo.

```
Router_DC#show ipv6 route static
Codes: C - Connected, L - Local, S - Static,
S   2001:A:B:10::/64 [1/0]
     via 2001:A:B:901::2
```

```
Router_DC#ping 2001:a:b:10:2050:79ff:fe66:680b
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to
2001:A:B:10:2050:79FF:FE66:680B, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
```

8.11. LAB08 – CẤU HÌNH GIAO THỨC ĐỊNH TUYẾN OSPFV3

Trong các hệ thống mạng thực tế, các vị trí quan trọng sẽ có nhiều kết nối nhằm đảm bảo tính dự phòng (Backup) và khả năng phân tán tải (Load-Sharing). Để thực hiện điều này cần phải sử dụng giao thức định tuyến động và giao thức được dùng phổ biến nhất là OSPF (Open Shortest Path First). Trong LAB này, chúng ta sẽ cấu hình OSPF trên ba router: Router_DC, Router_B1 và Router_B2. OSPF sẽ giúp tự động thiết lập các đường đi dự phòng và phân phối lưu lượng giữa hai đường truyền kết nối từ Site_B đến trung tâm dữ liệu.



Hình 129. Mô hình của bài LAB về OSPFv3

Phiên bản OSPF hỗ trợ IPv4 trước đây là OSPFv2, để khai báo cho IPv6 thì chúng ta phải sử dụng OSPFv3, là phiên bản cải tiến OSPFv2 nhưng hai phiên bản này không tương thích nhau. Nếu hệ thống chạy Dual Stack thì cần phải khai báo cả OSPFv2 cho IPv4 và OSPFv3 cho IPv6. Một yêu cầu nữa là dù khai báo OSPFv3 cho IPv6 thì chúng ta phải khai báo Router-ID là địa chỉ IPv4.

Dưới đây là cấu hình OSPF cho Router_DC và Router_B1, cấu hình cho Router_B2 tương tự.

```
Router_DC#show running-config
interface Loopback0
 ip address 10.255.255.1 255.255.255.255
 ipv6 address 2001:A:B::1/128
!
interface Ethernet1/1
ipv6 address 2001:A:B:902::1/126
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface Ethernet1/2
 ipv6 address 2001:A:B:903::1/126
 ipv6 enable
 ipv6 ospf 1 area 0
!
router ospfv3 1
 router-id 10.255.255.1
 !
 address-family ipv6 unicast
  redistribute connected    Thực hiện Redistribute
  redistribute static
 exit-address-family
```

```
Router_B1#show running-config
interface Loopback0
 ip address 10.255.255.20 255.255.255.255
 ipv6 address 2001:A:B::20/128
!
interface Ethernet0/0
 ipv6 address 2001:A:B:902::2/126
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface Ethernet0/1
 ipv6 address 2001:A:B:20::2/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
router ospfv3 1
 router-id 10.255.255.20
 !
 address-family ipv6 unicast
  passive-interface Ethernet0/1   Khai báo Passive Interface
 exit-address-family
```

Trong cấu hình ở trên, các địa chỉ của các Interface (Connected) và các Static Route được chuyển đổi (Redistribute) thành OSPF Route để quảng bá cho các router khác. Một số Interface không bật OSPF thì được cấu hình Passived-Interface. Tùy theo thực tế chúng ta có thể thay đổi cấu hình tương ứng.

Dưới đây là nội dung kiểm tra hoạt động của OSPFv3 tương ứng với cấu hình ở trên. Các router đều thiết lập IPv6 Neighbor ở trạng thái Full nhưng Neighbor ID vẫn là địa chỉ IPv4.

```
Router_DC#show ipv6 ospf neighbor
Neighbor ID     Pri   State           Dead Time
Interface ID    Interface
10.255.255.22     1   FULL/DR         00:00:35    3
Ethernet1/2
10.255.255.21     1   FULL/DR         00:00:36    3
Ethernet1/1
```

```
Router_B1#show ipv6 ospf neighbor
Neighbor ID     Pri   State           Dead Time
Interface ID    Interface
10.255.255.1      1   FULL/BDR        00:00:33    8
Ethernet0/0
```

```
Router_B2#show ipv6 ospf neighbor
Neighbor ID     Pri   State           Dead Time
Interface ID    Interface
10.255.255.1      1   FULL/BDR        00:00:37    9
Ethernet0/0
```

Kiểm tra Route IPv6 học qua OSPF trên Router_DC, thấy rằng router này đã học được Route 2001:A:B:20::/64 thuộc mạng LAN của Site_B qua cả 2 hướng là Ethernet1/1 và Ethernet1/2. Như vậy OSPF bảo đảm việc Backup và Load-Sharing tự động qua hai hướng.

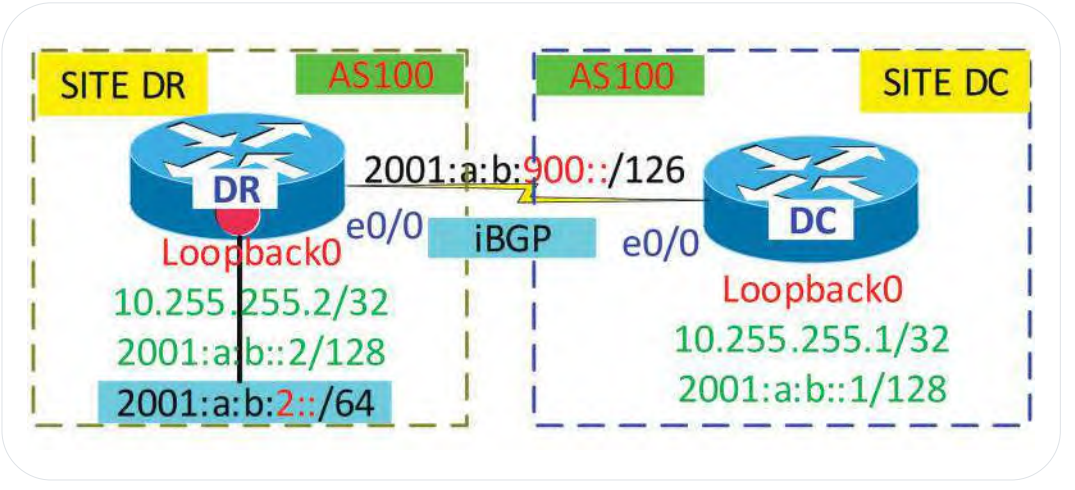
```
Router_DC#show ipv6 route ospf
Codes: O - OSPF Intra, OI - OSPF Inter
O   2001:A:B:20::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:8000, Ethernet1/1
     via FE80::A8BB:CCFF:FE00:9000, Ethernet1/2
```

Kiểm tra kết nối từ Router_DC đến máy tính thuộc mạng LAN của Site_B.

```
Router_DC#ping 2001:a:b:20:2050:79ff:fe66:680c
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to
2001:A:B:20:2050:79FF:FE66:680C, timeout is
2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/9/31 ms
```

8.12. LAB09 - CẤU HÌNH GIAO THỨC ĐỊNH TUYẾN IBGP

BGP (Border Gateway Protocol) là giao thức định tuyến duy nhất của mạng Internet cho phép kiểm soát các chính sách định tuyến linh hoạt và chặt chẽ giữa các hệ thống mạng tự quản (AS-Autonomous System) trên Internet. BGP được chia làm hai loại tùy theo phạm vi hoạt động đó là iBGP và eBGP. iBGP chỉ hoạt động giữa các router trong cùng AS trong khi đó eBGP dùng để trao đổi thông tin giữa các AS với nhau.



Hình 130. Mô hình của bài LAB về iBGP

Bài LAB này sẽ tập trung vào cấu hình iBGP giữa Router_DC và Router_DR, cả hai đều cùng thuộc AS100. Địa chỉ của Interface Loopback được dùng để Peering giữa các router nhằm đảm bảo tính ổn định và dự phòng cho kết nối đa hướng trong tương lai. Vì thế lệnh next-hop-self sẽ được sử dụng để quảng bá chính xác các router học được từ bên ngoài (học qua eBGP) nếu có cho các iBGP Peer bên trong (vì quảng bá qua iBGP thì Next-hop ban đầu sẽ không thay đổi). Lệnh network được dùng để quảng bá các Route nội bộ qua BGP.

```
Router_DC#show running-config
router bgp 100
 bgp router-id 10.255.255.1
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 2001:A:B::2 remote-as 100
 neighbor 2001:A:B::2 update-source Loopback0
 !
 address-family ipv6
  neighbor 2001:A:B::2 activate
  neighbor 2001:A:B::2 next-hop-self
 exit-address-family                    Đổi Nexthop khi quảng bá Route học từ các ISP
!
ipv6 route 2001:A:B::2/128 2001:A:B:900::2
!
     Khai static-route cho loopback để làm Peering Source
```

```
Router_DR#show running-config
router bgp 100
 bgp router-id 10.255.255.2
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 2001:A:B::1 remote-as 100
 neighbor 2001:A:B::1 update-source Loopback0
 !                                  Quảng bá Network  LAN qua BGP
 address-family ipv6
  network 2001:A:B:2::/64
  neighbor 2001:A:B::1 activate
  neighbor 2001:A:B::1 next-hop-self
 exit-address-family
!
ipv6 route 2001:A:B::1/128 2001:A:B:900::1
```

Sau khi cấu hình cần kiểm tra trạng thái hoạt động của BGP Neighbor:

```
Router_DC#show bgp ipv6 unicast summary
BGP router identifier 10.255.255.1, local AS number 100
BGP table version is 2, main routing table version 2
Neighbor        V           AS MsgRcvd MsgSent   TblVer
InQ OutQ Up/Down  State/PfxRcd
2001:A:B::2     4          100      58      58        2
0    0 00:48:19        1          Số Prefix nhận được
```

Kiểm tra IPv6 Route quảng bá từ Router_DR:

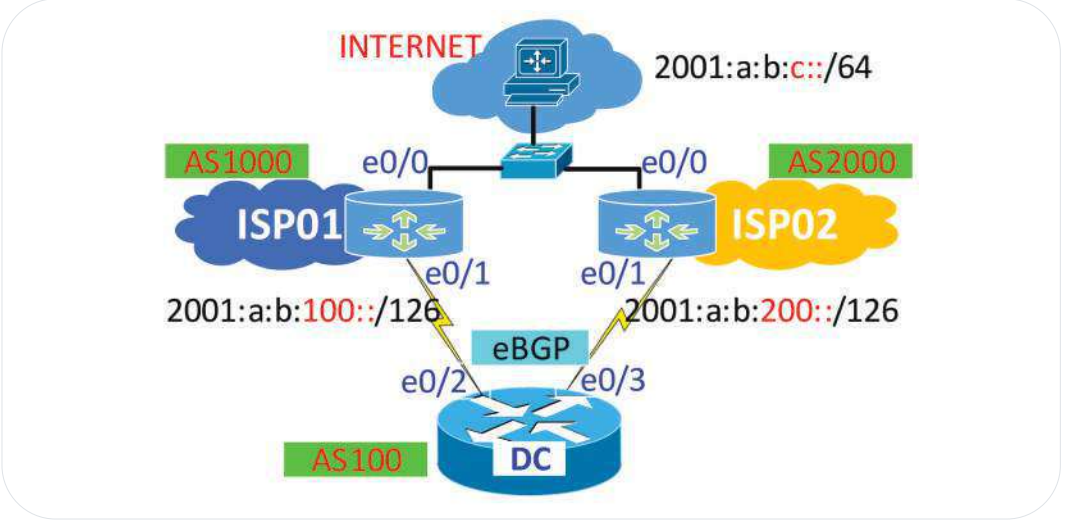
```
Router_DC#show ipv6 route bgp
IPv6 Routing Table - default - 18 entries
Codes: C - Connected, S - Static, B - BGP
B   2001:A:B:2::/64 [200/0]
     via 2001:A:B::2
```

Kiểm tra kết nối đến máy tính thuộc mạng LAN của Site DR:

```
Router_DC#ping  2001:a:b:2:2050:79ff:fe66:680a
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to
2001:A:B:2:2050:79FF:FE66:680A, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

8.13. LAB10 - CẤU HÌNH GIAO THỨC ĐỊNH TUYẾN eBGP

Khác với iBGP thì eBGP được sử dụng cho việc trao đổi định tuyến giữa các hệ thống mạng có AS khác nhau. Một số hoạt động của iBGP và eBGP cũng khác nhau ví dụ như iBGP yêu cầu phải Peering Full-Mesh, iBGP nhận Route từ Peer này sẽ không trao đổi với Peer kia, không thêm ASN, một số thuộc tính nhận được từ eBGP sẽ không được xử lý hoặc chuyển tiếp trong iBGP ... Vì thế cần tìm hiểu kỹ hoạt động của hai loại giao thức định tuyến BGP này.



Hình 131. Mô hình của bài LAB về eBGP

Trong bài LAB này, chúng ta sẽ tiến hành khai báo eBGP trên Router_DC, kết nối Multi-Homing với ISP01 và ISP02. Sẽ có một máy tính kết nối với cả ISP01 và ISP02 để kiểm tra kết nối sau khi cấu hình eBGP.

Dưới đây là cấu hình eBGP trên Router_DC.

```
Router_DC#show running-config
interface Ethernet0/2
 description To_ISP01
 ipv6 address 2001:A:B:100::1/126
 ipv6 enable
!
interface Ethernet0/3
 description To_ISP02
 ipv6 address 2001:A:B:200::1/126
 ipv6 enable
!
router bgp 100
 bgp router-id 10.255.255.1
 no bgp default ipv4-unicast
 neighbor 2001:A:B:100::2 remote-as 1000
 neighbor 2001:A:B:200::2 remote-as 2000
 network  2001:A:B::1/128        Quảng bá địa chỉ Loopback qua BGP
 !
 address-family ipv6
  neighbor 2001:A:B:100::2 activate
  neighbor 2001:A:B:200::2 activate
 exit-address-family
```

Tương tự là cấu hình của ISP01 và ISP02

```
ISP01#show running-config
interface Ethernet0/0
 description To_Internet
 ipv6 address 2001:A:B:C::2/64
 vrrp 1 address-family ipv6
  priority 110
  address FE80::12:1 primary
  address 2001:A:B:C::1/64
  exit-vrrp
!
interface Ethernet0/1
 description To_Router_DC
 ipv6 address 2001:A:B:100::2/126
!
router bgp 1000
 bgp router-id 10.255.255.100
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 2001:A:B:100::1 remote-as 100
 !
 address-family ipv6
  network 2001:A:B:C::/64
  neighbor 2001:A:B:100::1 activate
 exit-address-family
```

```
ISP02#show running-config
interface Ethernet0/0
 description To_Internet
 ipv6 address 2001:A:B:C::3/64
 vrrp 1 address-family ipv6
  address FE80::12:1 primary
  address 2001:A:B:C::1/64
  exit-vrrp
!
interface Ethernet0/1
 description To_Router_DC
 ipv6 address 2001:A:B:200::2/126
!
router bgp 2000
 bgp router-id 10.255.255.200
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 2001:A:B:200::1 remote-as 100
 !
 address-family ipv6
  network 2001:A:B:C::/64
  neighbor 2001:A:B:200::1 activate
 exit-address-family
```

Sau đây là kiểm tra kết quả hoạt động khai báo cho eBGP cho các thiết bị. Trên Router_DC đã thiết lập thành công phiên BGP đến ISP01 và ISP02.

```
Router_DC#show bgp ipv6 unicast summary
BGP router identifier 10.255.255.1, local AS number 100
Neighbor        V           AS MsgRcvd MsgSent   TblVer
InQ OutQ Up/Down  State/PfxRc
d
2001:A:B::2     4          100    1474    1468        3
0    0 22:11:59        1
2001:A:B:100::2 4         1000       5       4        2
0    0 00:00:19        1
2001:A:B:200::2 4         2000       5       5        2
0    0 00:00:21        1
```

```
Router_DC#show ipv6 route bgp
IPv6 Routing Table - default - 18 entries
Codes: C - Connected, S - Static, B - BGP
B   2001:A:B:2::/64 [200/0]
     via 2001:A:B::2
B   2001:A:B:C::/64 [20/0]
     via FE80::A8BB:CCFF:FE00:A10, Ethernet0/3
```

Kiểm tra kết nối từ Router_DC đến máy tính đại diện trên Internet:

```
Router_DC#ping 2001:a:b:c:2050:79ff:fe66:6804
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to
2001:A:B:C:2050:79FF:FE66:6804, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/11 ms
```

Như vậy kết nối giữa các thiết bị thông qua eBGP đã hoạt động tốt sau cấu hình.

Chú ý:

- Trong bài LAB trên có cả cấu hình cho VRRP trên ISP01 và ISP02. Đây là mô hình giả lập để Router_DC có thể Ping tới máy tính đại diện trên Internet, trong thực tế sẽ không có cấu hình VRRP này.

8.14. TỔNG KẾT CHƯƠNG 8

Chương 8 đã cung cấp hướng dẫn chuyên sâu về triển khai **IPv6 Dual Stack**, một giải pháp chiến lược cho phép vận hành đồng thời IPv6 trên hạ tầng IPv4 hiện có, đảm bảo không làm gián đoạn dịch vụ và giảm thiểu sự phụ thuộc vào IPv4. Nội dung chương tập trung vào mô hình mạng với **IP/ASN độc lập**, một mô hình tối ưu, cung cấp các kịch bản triển khai toàn diện để bạn đọc nắm bắt đầy đủ các khía cạnh của Dual Stack.

Chương 8 đã trình bày chi tiết các bài thực hành (LAB), bao gồm cấu hình địa chỉ IPv6 **tĩnh** và **động** trên router, hệ điều hành Windows, Ubuntu, sử dụng các phương thức như **SLAAC, Stateful DHCPv6 và Stateless DHCPv6**. Ngoài ra, chương cũng hướng dẫn cấu hình các giao thức quan trọng như VRRPv3 để đảm bảo tính dự phòng, cùng với các phương pháp định tuyến tĩnh và động (bao gồm OSPFv3, iBGP và eBGP). Việc triển khai IPv6 Dual Stack tạo điều kiện cho quá trình chuyển đổi từ IPv4 sang IPv6 diễn ra suôn sẻ, đảm bảo khả năng kết nối linh hoạt mà không làm gián đoạn hệ thống mạng hiện tại.

8.15. CÂU HỎI ÔN TẬP CHƯƠNG 8

Chương này tập trung giải quyết vấn đề gì trong việc triển khai IPv6 cho các hệ thống mạng? Đối tượng chính mà nội dung chương này hướng đến là ai?

01 Chương này tập trung vào vấn đề triển khai thực tế IPv6 theo mô hình Dual Stack cho các hệ thống mạng. Nội dung được thiết kế đặc biệt dành cho các tổ chức và doanh nghiệp sở hữu địa chỉ IP và ASN độc lập. Mục tiêu là giúp các đơn vị này xây dựng một hạ tầng mạng hiện đại, bảo mật và đáp ứng các yêu cầu mở rộng trong tương lai

Làm thế nào để các thiết bị trong mạng Dual Stack nhận địa chỉ IPv6?

02 Các thiết bị trong mạng Dual Stack có thể nhận địa chỉ IPv6 thông qua nhiều phương pháp khác nhau:

- **Cấu hình tĩnh:** Địa chỉ IPv6 được cấu hình thủ công trên từng thiết bị.
- **SLAAC (Stateless Address Autoconfiguration):** Các thiết bị tự động tạo địa chỉ IPv6 cho mình dựa trên tiền tố mạng (Prefix) được quảng bá bởi router thông qua bản tin RA (Router Advertisement) và một Interface ID được tạo bằng EUI-64 hoặc ngẫu nhiên.
- **DHCPv6:Stateful DHCPv6:** Một máy chủ DHCPv6 quản lý việc cấp phát địa chỉ IPv6, DNS server và các thông tin cấu hình khác cho các thiết bị, đồng thời lưu trữ trạng thái của các địa chỉ đã cấp.
- **Stateless DHCPv6:** Các thiết bị tự động cấu hình địa chỉ IPv6 bằng SLAAC, nhưng sử dụng DHCPv6 Server để nhận các thông tin cấu hình bổ sung như địa chỉ DNS server và tên miền.

IP độc lập (PI) và số hiệu mạng ASN mang lại lợi ích gì?

03 Địa chỉ IP độc lập (Provider Independent) cho phép các tổ chức và doanh nghiệp tự do lựa chọn kết nối mạng của mình với bất kỳ nhà mạng nào mà không lo bị gián đoạn dịch vụ khi thay đổi nhà mạng. Số hiệu mạng ASN (Autonomous System Number) đóng vai trò là "định danh chủ thể" của một hệ thống mạng trên Internet và cần thiết để quản lý các dãy địa chỉ IP độc lập. ASN cũng là một thuộc tính quan trọng của giao thức định tuyến BGP, giúp xây dựng chính sách định tuyến và chọn đường đi tốt nhất giữa các hệ thống mạng. Kết hợp IP độc lập và ASN giúp các tổ chức tự chủ hơn trong việc quản lý mạng, bảo mật và tối ưu hóa kết nối Internet.

Kết nối đa hướng (Multi-homing) được triển khai như thế nào trong môi trường IPv6 Dual Stack và lợi ích của nó là gì?

04 Kết nối đa hướng (Multi-homing) trong môi trường IPv6 Dual Stack được triển khai bằng cách thiết lập đồng thời kết nối với nhiều nhà cung cấp dịch vụ Internet (ISP). Khi một ISP gặp sự cố, hệ thống sẽ tự động chuyển mạch lưu lượng sang các kết nối còn lại, đảm bảo tính sẵn sàng cao và dịch vụ không bị gián đoạn. Multi-homing cũng cho phép lựa chọn tuyến đường tối ưu nhất để đến đích, giúp cải thiện tốc độ truy cập Internet. Việc sử dụng IP độc lập (PI) và ASN tạo điều kiện thuận lợi cho việc triển khai Multi-homing hiệu quả.

Giao thức VRRPv3 được sử dụng để làm gì trong mạng IPv6 Dual Stack và nó hoạt động như thế nào?

05 VRRP (Virtual Router Redundancy Protocol) là một giao thức dự phòng cho phép nhiều router hoạt động như một router ảo, tăng cường tính sẵn sàng cho default gateway trong mạng. Đối với IPv6, cần sử dụng phiên bản VRRPv3, phiên bản này hỗ trợ cả IPv4 và IPv6. VRRPv3 hoạt động bằng cách bầu chọn một router chủ (Master) chịu trách nhiệm chuyển tiếp lưu lượng, trong khi các router dự phòng (Backup) sẽ giám sát trạng thái của router chủ và sẵn sàng tiếp quản nếu router chủ gặp sự cố. VRRPv3 sử dụng địa chỉ Link-Local ảo và địa chỉ Unicast ảo để các thiết bị trong mạng có thể sử dụng làm default gateway.

06 Các giao thức định tuyến động như OSPFv3 và BGP được cấu hình như thế nào trong môi trường IPv6 Dual Stack và vai trò của chúng là gì?

- **OSPFv3 (Open Shortest Path First version 3):** Là một giao thức định tuyến link-state được sử dụng để trao đổi thông tin định tuyến trong cùng một vùng mạng (Autonomous System). OSPFv3 hỗ trợ IPv6 và giúp các router tự động tìm ra đường đi ngắn nhất và thiết lập các đường đi dự phòng. Khi cấu hình OSPFv3, cần gán một Router-ID (thường là địa chỉ IPv4) và chỉ định các interface tham gia vào các vùng (area).
- **BGP (Border Gateway Protocol):** Là giao thức định tuyến duy nhất của Internet, được sử dụng để trao đổi thông tin định tuyến giữa các Autonomous System (AS). BGP được chia thành iBGP (Internal BGP) sử dụng trong cùng một AS và eBGP (External BGP) sử dụng giữa các AS khác nhau. Khi cấu hình iBGP, các router trong cùng một AS thiết lập quan hệ láng giềng (peering) để trao đổi thông tin định tuyến nội bộ. Khi cấu hình eBGP, các router giữa các AS khác nhau thiết lập peering để trao đổi thông tin định tuyến Internet.

07 Sự khác biệt giữa Stateful DHCPv6 và Stateless DHCPv6 là gì và khi nào nên sử dụng loại nào?

- **Stateful DHCPv6:** Máy chủ DHCPv6 cấp phát địa chỉ IPv6, DNS server và các thông tin cấu hình khác cho client, đồng thời quản lý trạng thái (địa chỉ IP đã cấp, thời gian thuê...). Phương pháp này phù hợp khi cần kiểm soát và theo dõi việc cấp phát địa chỉ IP, ví dụ trong các mạng doanh nghiệp lớn.
- **Stateless DHCPv6:** Client tự động cấu hình địa chỉ IPv6 bằng SLAAC, sau đó gửi yêu cầu đến DHCPv6 server để nhận các thông tin cấu hình bổ sung như DNS server và tên miền. Máy chủ DHCPv6 không quản lý việc cấp phát địa chỉ IP. Phương pháp này phù hợp cho các mạng lớn, phức tạp, giúp giảm tải cho máy chủ DHCP và tận dụng tính năng tự động cấu hình của SLAAC.

08 Các bài LAB trong chương 8 cung cấp những nội dung thực hành quan trọng nào cho việc triển khai IPv6 Dual Stack?

- Các bài LAB trong chương 8 cung cấp các nội dung thực hành chi tiết và quan trọng cho việc triển khai IPv6 Dual Stack, bao gồm:
- Cấu hình địa chỉ IPv6 tĩnh trên router, Windows và Ubuntu.
- Cấu hình địa chỉ IPv6 động bằng SLAAC.
- Cấu hình địa chỉ IPv6 động bằng Stateful DHCPv6 và Stateless DHCPv6.
- Cấu hình giao thức dự phòng VRRPv3.
- Cấu hình định tuyến tĩnh (Static Route) cho IPv6.
- Cấu hình giao thức định tuyến động OSPFv3.
- Cấu hình giao thức định tuyến iBGP và eBGP để kết nối giữa các AS.

Thông qua các bài LAB này, người đọc có thể nắm vững các kỹ năng cơ bản và nâng cao để triển khai và quản lý hiệu quả mạng Dual Stack trong các tình huống thực tế.

PHẦN 2 – THỰC HÀNH

CHƯƠNG 9

HƯỚNG DẪN TRIỂN KHAI MÔ HÌNH IPv6 ONLY

Mô hình mạng IPv6 Only được xem là giải pháp chiến lược và bền vững vì không chỉ giải quyết triệt để vấn đề cạn kiệt địa chỉ IPv4 mà còn loại bỏ sự phức tạp khi phải duy trì song song cả hai giao thức. Với khả năng đơn giản hóa hạ tầng, tối ưu công tác vận hành và đáp ứng khả năng mở rộng trong tương lai, IPv6 Only đang dần trở thành xu hướng được áp dụng rộng rãi trên thế giới. Tuy nhiên, thách thức lớn nhất khi triển khai IPv6 Only là đảm bảo khả năng kết nối liền mạch với các hệ thống, dịch vụ và ứng dụng vẫn hoạt động với IPv4.

Chương 9 tập trung vào hướng dẫn triển khai mô hình mạng IPv6 Only, tập trung cho mạng doanh nghiệp và các trung tâm dữ liệu với giải pháp chính là kết hợp giữa NAT64 và DNS64. Chương này hướng dẫn chi tiết các bước cấu hình NAT64 trên Router Cisco và triển khai DNS64 bằng phần mềm BIND. Một giải pháp khác cũng được trình bày là tích hợp cả hai chức năng này trên một hệ thống Linux bằng cách sử dụng thêm phần mềm Jool.

CÁC NỘI DUNG CỦA CHƯƠNG NÀY GỒM:

Lý do, lợi ích và thách thức khi triển khai IPv6 Only.

Hướng dẫn chi tiết các bước triển khai giải pháp DNS64/NAT64 cho **mạng doanh nghiệp và trung tâm dữ liệu**.

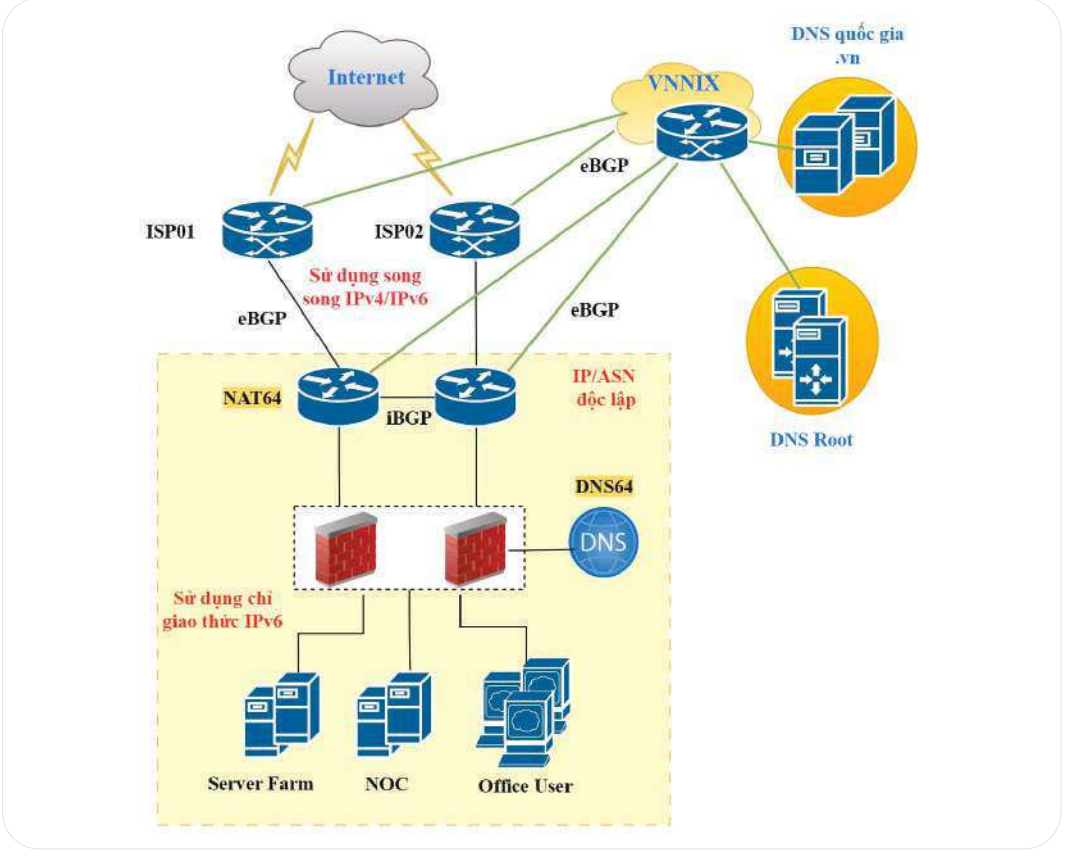
Một số **hạn chế** của giải pháp DNS64/NAT64.

Hai mô hình LAB chính được trình bày:

- **Mô hình độc lập:** Chức năng NAT64 và DNS64 hoạt động trên hai thiết bị khác nhau, tận dụng tính năng NAT64 trên router và triển khai DNS64 trên máy chủ độc lập.
- **Mô hình tích hợp:** Cả hai chức năng DNS64 và NAT64 được tích hợp trên cùng một máy chủ Linux sử dụng phần mềm BIND cho DNS64 và Jool cho NAT64.

9.1. MÔ HÌNH MẠNG TIÊN TIẾN IPv6 ONLY CHO DOANH NGHIỆP, CƠ QUAN VÀ TỔ CHỨC VỚI DNS64 VÀ NAT64

Như đã trình bày trong phần lý thuyết, mô hình mạng IPv6 Only là giải pháp tiên tiến giúp các doanh nghiệp, cơ quan và tổ chức xây dựng hạ tầng mạng hiện đại, tối ưu hóa hiệu suất và bảo mật, sẵn sàng cho các công nghệ như IoT, 5G và Cloud Computing. Mô hình LAB ở chương này cũng kế thừa mô hình Dual Stack ở chương trước, sử dụng IP/ASN độc lập để tự quản lý định tuyến qua giao thức BGP, đồng thời hoạt động hoàn toàn trên giao thức IPv6, loại bỏ sự phụ thuộc vào IPv4. Để đảm bảo khả năng giao tiếp với các tài nguyên IPv4 vẫn tồn tại trên Internet, DNS64 được triển khai nhằm phân giải tên miền, tạo địa chỉ IPv6 tổng hợp cho các thiết bị IPv6 Only, trong khi NAT64 chuyển đổi lưu lượng từ IPv6 sang IPv4 tại điểm biên, duy trì kết nối liền mạch với mạng Internet toàn cầu.



Hình 132. Mô hình mạng hiện đại với IP/ASN độc lập và kết nối đa hướng

Phần thực hành chương này hướng dẫn chi tiết cách triển khai mô hình mạng IPv6 Only, với các bài LAB tập trung chuyên sâu về thiết lập DNS64 và NAT64, giúp các doanh nghiệp và cơ quan có nhu cầu chuyển đổi hoàn toàn sang IPv6.

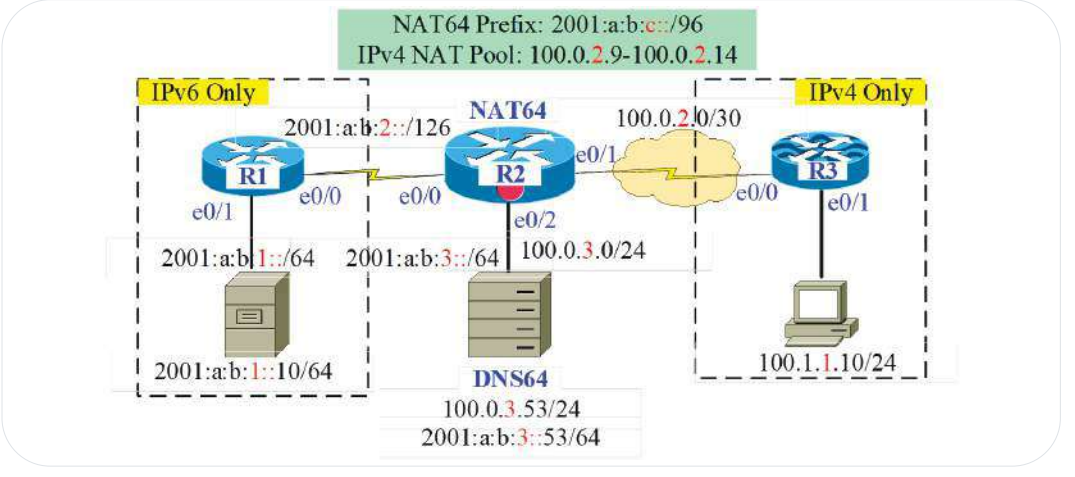
Chú ý:
- Nội dung chương này tập trung vào các khai báo cho DNS64 và NAT64. Việc khai báo IPv6 cho các giao thức như Static Route, SLAAC, DHCP, VRRPv3, OSPFv3 và BGP hoàn toàn giống như trong chương 9 nên sẽ không được trình bày ở đây.

9.2. MÔ HÌNH VÀ NỘI DUNG LAB IPv6 ONLY

Nội dung thực hành của chương này bao gồm hai mô hình LAB, được thiết kế phù hợp với các đặc điểm kỹ thuật của các hệ thống mạng thực tế:

Mô hình 01 (độc lập)

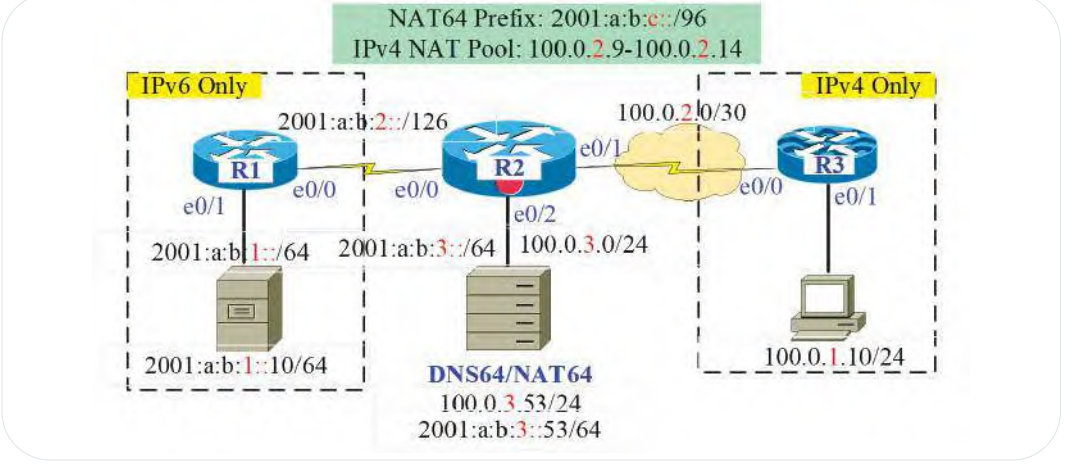
Trong mô hình này, chức năng của NAT64 và DNS64 được tách riêng, hoạt động độc lập trên hai thiết bị khác nhau. Trong thực tế, một số thiết bị router của các doanh nghiệp hiện nay đã hỗ trợ tính năng NAT64. Do đó, mô hình tận dụng tính năng này để cấu hình NAT64 trực tiếp trên router nhằm tập trung vào quản lý định tuyến, đồng thời đảm bảo hiệu suất và độ ổn định cao hơn. Dịch vụ DNS64 được triển khai riêng trên một máy chủ độc lập.



Hình 133. Mô hình LAB IPv6 Only với NAT64 và DNS64 độc lập

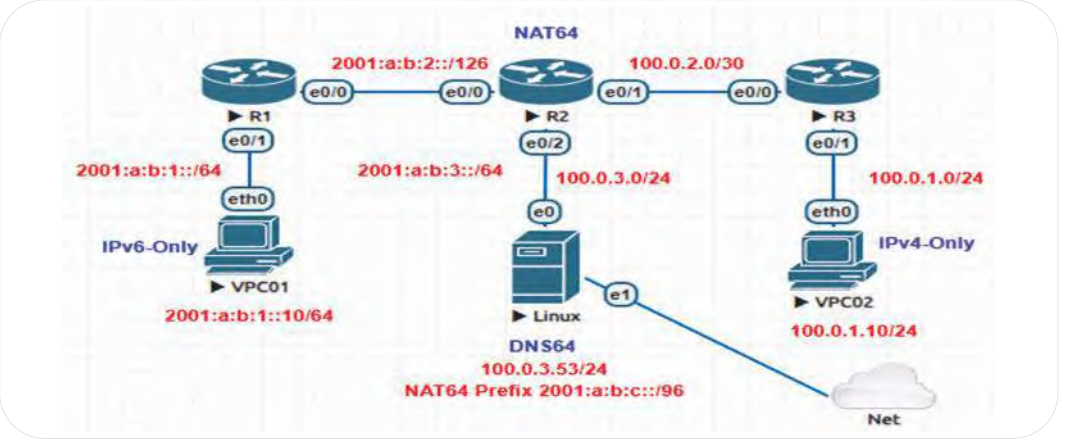
Trong mô hình 02 (tích hợp)

Trong mô hình 02 (tích hợp): Cả hai chức năng DNS64 và NAT64 tích hợp trên cùng một máy chủ, hoạt động song song. Mô hình này phù hợp với các hệ thống mạng dù có router nhưng không hỗ trợ NAT64 nhưng vẫn muốn thử nghiệm hoặc triển khai chuyển đổi sang IPv6 Only. Chúng ta sử dụng phần mềm BIND cho DNS64 và Jool cho NAT64, cả hai là đều là phần mềm mã nguồn mở được dùng phổ biến và đáng tin cậy. Việc này sẽ giúp các doanh nghiệp tiết kiệm chi phí và chủ động triển khai, không phụ thuộc vào việc nâng cấp tính năng hay thay thế router hiện có.



Hình 134. Mô hình LAB IPv6 Only với NAT64 và DNS64 được tích hợp

Toàn bộ các nội dung LAB được thực hành trên phần mềm EVE-NG với R1, R2 và R3 là Cisco Router IOL còn DNS64 sử dụng Ubuntu phiên bản 16.4. Để có thể cài đặt các phần mềm trên Ubuntu thì cần có 2 Card mạng, trong đó một Card mạng kết nối với Cloud0 (Management) để kết nối ra Internet theo mô hình bên dưới. Các máy tính nối R1 và R3 là các VPC sẵn có trong EVE-NG.



Hình 135. Mô hình LAB trên phần mềm EVE-NG

Mục tiêu của 2 mô hình LAB là các máy tính IPv6 Only thuộc R1 có thể truy cập được máy tính IPv4 Only thuộc R3 thông qua tính năng NAT64 và DNS64.

9.3. CÁC BÀI LAB CHI TIẾT CHO MÔ HÌNH IPv6 ONLY

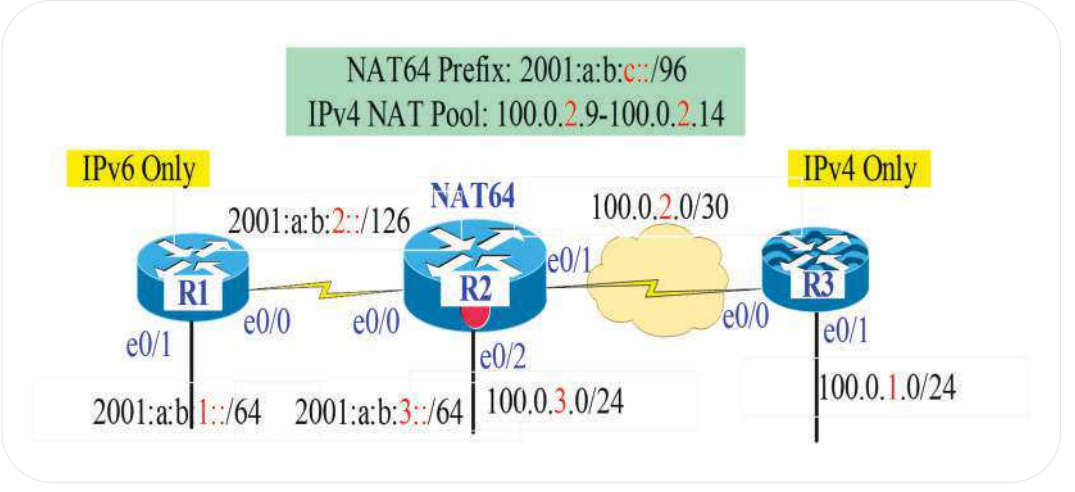
Hai mô hình trên bao gồm nhiều bài LAB chi tiết, được thiết kế nhằm hỗ trợ quá trình triển khai mạng IPv6 Only một cách hiệu quả và linh hoạt, phù hợp với nhiều kịch bản thực tế. Các bài LAB bao gồm: từ sử dụng Dynamic NAT64 cho kết nối Outbound, Overload NAT64 để tối ưu hóa lưu lượng, Static NAT64 cho kết nối Inbound, đến các cấu hình Resolver và Authoritative Server cho DNS64. Đặc biệt là bài LAB tích hợp giữa NAT64 và DNS64 mang lại giải pháp tiết kiệm chi phí và dễ dàng tùy chỉnh với sự hỗ trợ từ các công cụ mã nguồn mở như BIND và Jool. Tùy thuộc vào nhu cầu và đặc điểm riêng của từng hệ thống, các bạn có thể linh hoạt áp dụng nhiều kịch bản LAB chi tiết này để tối ưu hóa quá trình chuyển đổi từ IPv4 sang IPv6 Only.

Mô hình	Bài LAB	Nội dung	Mục đích
Mô hình độc lập	LAB01	Sử dụng Dynamic NAT64 cho Outbound NAT	Dành cho kết nối từ mạng IPv6 Only truy cập ra các máy tính IPv4 Only bên ngoài theo mô hình NAT động 1:1
	LAB02	Sử dụng Overload NAT64 cho Outbound NAT	Dành cho kết nối từ mạng IPv6 Only truy cập ra các máy tính IPv4 Only bên ngoài theo mô hình NAT động N:1
	LAB03	Sử dụng Static NAT64 cho Inbound NAT	Hỗ trợ cho nhu cầu các máy tính mạng IPv6 cung cấp dịch vụ cho máy tính IPv4 bên ngoài truy cập vào
	LAB04	Sử dụng DNS64 Server chế độ IPv6 Only làm Resolver cho kết nối Outbound	Server DNS64 làm nhiệm vụ phân giải tên miền cho các kết nối từ IPv6 ra mạng IPv4 bên ngoài (dành cho Outbound NAT)
	LAB05	Kiểm tra hoạt động của DNS64 và NAT64 mô hình độc lập cho kết nối Outbound	Kiểm tra sự kết hợp hoạt động giữa NAT64 và DNS64 cho kết nối từ mạng IPv6 ra các máy tính IPv4 bên ngoài
	LAB06	Sử dụng DNS64 chế độ Dual Stack làm Authoritative Server cho kết nối Inbound	Server DNS64 đóng vai trò Authoritative Server cho máy tính IPv6 và IPv4 bên ngoài truy cập vào máy chủ IPv6 bên trong (dành cho Inbound NAT)
Mô hình độc lập	LAB07	Mô hình tích hợp DNS64/NAT64	Tính năng NAT64 và DNS64 sẽ được tích hợp trên cùng một máy chủ Linux, không cần router hỗ trợ NAT64

Bảng 15. Các bài LAB chi tiết kết hợp giữa NAT64 và DNS64

9.4. LAB01- SỬ DỤNG DYNAMIC NAT64 CHO OUTBOUND NAT

Trong bài LAB này, chúng ta cấu hình tính năng NAT64 trên Router R2 và kiểm tra hoạt động sau khi cấu hình. Địa chỉ đích IPv4 được chuyển đổi sang địa chỉ IPv6 bằng cách thêm NAT64 Prefix là **2001:a:b:c::/96**. Đồng thời, các địa chỉ nguồn từ mạng IPv6 Only sẽ được NAT sang địa chỉ IPv4 nằm trong Pool có tên **POOLv4**, với dãy địa chỉ từ **100.1.2.9** đến **100.0.2.14**. Dưới đây là cấu hình chi tiết cho các router.



Hình 136. Mô hình của bài LAB về Dynamic NAT64

Trên R1 chỉ cấu hình địa chỉ và Route IPv6.

```
R1#show running-config
ipv6 unicast-routing
!
interface Ethernet0/0
 ipv6 address 2001:A:B:2::1/126
!
interface Ethernet0/1
 ipv6 address 2001:A:B:1::1/64
!
ipv6 route ::/0 2001:A:B:2::2
```

Trên R3 chỉ cấu hình địa chỉ và Route IPv4.

```
R3#show running-config
!
interface Ethernet0/0
 ip address 100.0.2.2 255.255.255.0
!
interface Ethernet0/1
 ip address 100.0.1.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 100.0.2.1
```

Dưới đây là cấu hình NAT64 trên R3. Đầu tiên bật tính năng NAT64 trên các Interface cần chuyển đổi từ IPv6 sang IPv4 và ngược lại.

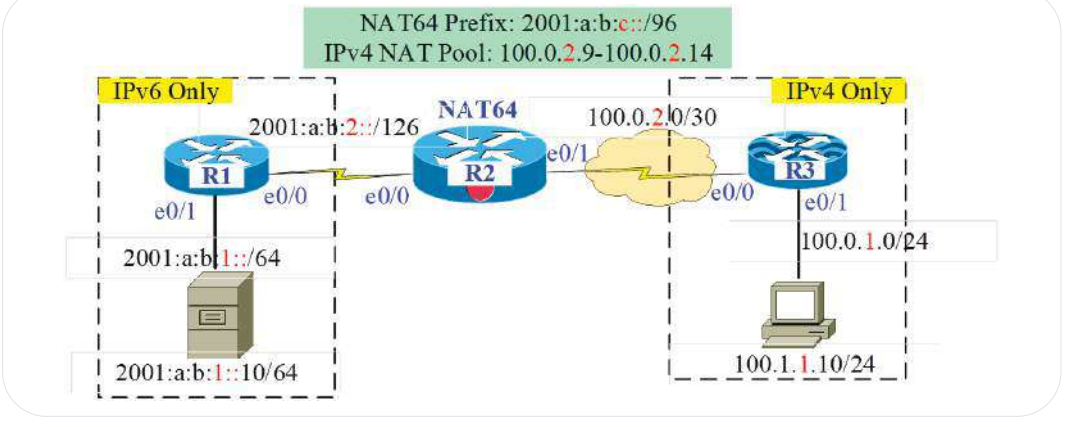
```
R2#show running-config
!
ipv6 unicast-routing
!
interface Ethernet0/0
 nat64 enable                                  Bật tính năng cho phép chuyển đổi giữa IPv6 và IPv4
 ipv6 address 2001:A:B:2::2/126
!
interface Ethernet0/1
 ip address 100.0.2.1 255.255.255.252
 nat64 enable
!
interface Ethernet0/2
 ip address 100.0.3.1 255.255.255.0
 ipv6 address 2001:A:B:3::1/64
!
ip route 100.0.1.0 255.255.255.0 100.0.2.2
!                                              Cấu hình liên quan NAT64
nat64 prefix stateful 2001:A:B:C::/96
nat64 v4 pool POOLv4 100.0.2.9 100.0.2.15
nat64 v6v4 list NAT64_ACL pool POOLv4
ipv6 route 2001:A:B:1::/64 2001:A:B:2::1
!
ipv6 access-list NAT64_ACL
 permit ipv6 any 2001:A:B:C::/96              Tất cả Traffic đi đến NAT64 Prefix
```

Để cấu hình NAT64, chúng ta cần khai báo các thông tin sau:

- **NAT64 Prefix:** Dãy địa chỉ IPv6 được sử dụng để chuyển đổi địa chỉ IPv4 sang IPv6, còn gọi là địa chỉ IPv4-Embedded IPv6.
- **IPv4 Pool:** Dãy địa chỉ IPv4 dùng để NAT địa chỉ IPv6 thành IPv4, hỗ trợ các thiết bị IPv6 Only truy cập đến các thiết bị IPv4 Only.
- **IPv6 Access-List:** Dùng để lọc và xác định các gói tin cần thực hiện NAT64. Access-List trong ví dụ này cho phép các gói tin từ mạng IPv6 đến các đích có địa chỉ chứa NAT Prefix, hay tức là các bản tin IPv6 đi đến đích IPv4.
- **Cấu hình NAT Mapping:** Kết hợp NAT64 Prefix, IPv4 Pool và Access-List để tạo ánh xạ giữa địa chỉ IPv6 và IPv4, đảm bảo luồng dữ liệu từ mạng IPv6 có thể chuyển đổi sang mạng IPv4.

Chú ý:

- Một chú ý ở đây là IPv4 NAT POOL không được cùng lớp mạng với địa chỉ của cổng kết nối với mạng IPv4, trong bài LAB này là cổng Ethernet0/1, nếu cùng thì kết nối sẽ không thành công.
- Trong bài LAB này, POOLv4 chạy từ 100.0.2.9 đến 100.0.2.14 không cùng dãy mạng với địa chỉ của cổng Ethernet0/1 là 100.0.2.0/30.



Hình 137. Mô hình kiểm tra của bài LAB về Dynamic NAT64

Thực hiện kiểm tra kết nối từ máy tính mạng IPv6 Only sang máy tính mạng IPv4 Only (địa chỉ 100.0.1.10/24). Chúng ta dùng lệnh PING kết hợp địa chỉ NAT64 Prefix + địa chỉ IPv4 của máy tính đích.

```
VPC01> ping 2001:a:b:c::100.0.1.10

2001:a:b:c::100.0.1.10 icmp6_seq=1 ttl=61 time=14.029 ms
2001:a:b:c::100.0.1.10 icmp6_seq=2 ttl=61 time=2.158 ms
2001:a:b:c::100.0.1.10 icmp6_seq=3 ttl=61 time=2.345 ms
2001:a:b:c::100.0.1.10 icmp6_seq=4 ttl=61 time=2.881 ms
2001:a:b:c::100.0.1.10 icmp6_seq=5 ttl=61 time=6.168 ms
```

Một cách khác, chúng ta đổi địa chỉ IPv4 từ thập phân sang bát phân (Hexa) rồi kết hợp với địa chỉ NAT64 Prefix rồi sau đó thực hiện lệnh PING. Ví dụ, địa chỉ IPv4 100.0.1.10 chuyển sang Hexa là 6400:10a, chúng ta có thể PING như sau:

```
VPC01> ping 2001:a:b:c::6400:10a

2001:a:b:c::6400:10a icmp6_seq=1 ttl=61 time=4.652 ms
2001:a:b:c::6400:10a icmp6_seq=2 ttl=61 time=2.091 ms
2001:a:b:c::6400:10a icmp6_seq=3 ttl=61 time=1.968 ms
2001:a:b:c::6400:10a icmp6_seq=4 ttl=61 time=4.304 ms
2001:a:b:c::6400:10a icmp6_seq=5 ttl=61 time=1.642 ms
```

Bài LAB này mới giới thiệu về cấu hình và kiểm tra hoạt động của NAT64, chưa sử dụng đến DNS64 vì chúng ta Ping trực tiếp địa chỉ thay vì Ping bằng tên miền.

Dưới đây là kiểm tra hoạt động của NAT64 trên R2:

```
R2#show nat64 translations
Proto       Original IPv4         Translated IPv4
            Translated IPv6       Original IPv6
------------------------------------------------------------------
udp         100.0.1.10:45474      [2001:A:B:C::6400:10A]:45474
            100.0.2.12:45473      [2001:A:B:1::10]:45473
--------------
            100.0.2.12            2001:A:B:1::10
udp         100.0.1.10:33437      [2001:A:B:C::6400:10A]:33437
            100.0.2.13:49446      [2001:A:B:2::1]:49446
--------------
            100.0.2.13            2001:A:B:2::1
```

Dòng lệnh cho thấy máy tính có địa chỉ IPv6 **2001:A:B:1::10** được NAT64 chuyển đổi thành địa chỉ IPv4 100.0.2.10 khi gửi dữ liệu sang mạng IPv4. Đồng thời, địa chỉ đích **2001:A:B:C::6400:10A** được loại bỏ phần NAT64 Prefix, chuyển thành địa chỉ IPv4 **100.0.1.10**. Lưu ý rằng các địa chỉ IPv6 được NAT động theo kiểu 1:1, ví dụ như **2001:A:B:1::10** ánh xạ thành **100.0.2.12** và **2001:A:B:2::1** ánh xạ thành **100.0.2.13**.

9.5. LAB02 – SỬ DỤNG OVERLOAD NAT64 CHO OUTBOUND NAT

Trong bài LAB trên, chúng ta đã cấu hình NAT Dynamic, trong đó mỗi địa chỉ IPv6 được ánh xạ 1:1 với một địa chỉ IPv4 trước khi truy cập ra bên ngoài. Tuy nhiên, để tiết kiệm địa chỉ IPv4, hoặc trong trường hợp số lượng máy tính IPv6 vượt quá số lượng địa chỉ IPv4 có trong NAT POOL, chúng ta cần thực hiện NAT theo cổng (Port). Phương pháp này tương tự như PAT (Port Address Translation) giữa IPv4 với IPv4, cho phép nhiều địa chỉ IPv6 được NAT chung qua một địa chỉ IPv4 duy nhất bằng cách sử dụng các cổng khác nhau.

Để thực hiện NAT64 Overload thì trên R2 chúng ta chỉ cần xóa dòng lệnh NAT64 cũ và nhập lại với cụm từ "Overload" được thêm vào.

```
nat64 prefix stateful 2001:A:B:C::/96
nat64 v4 pool POOLv4 100.0.2.9 100.0.2.15
nat64 v6v4 list NAT64_ACL pool POOLv4 overload
ipv6 route 2001:A:B:1::/64 2001:A:B:2::1
```

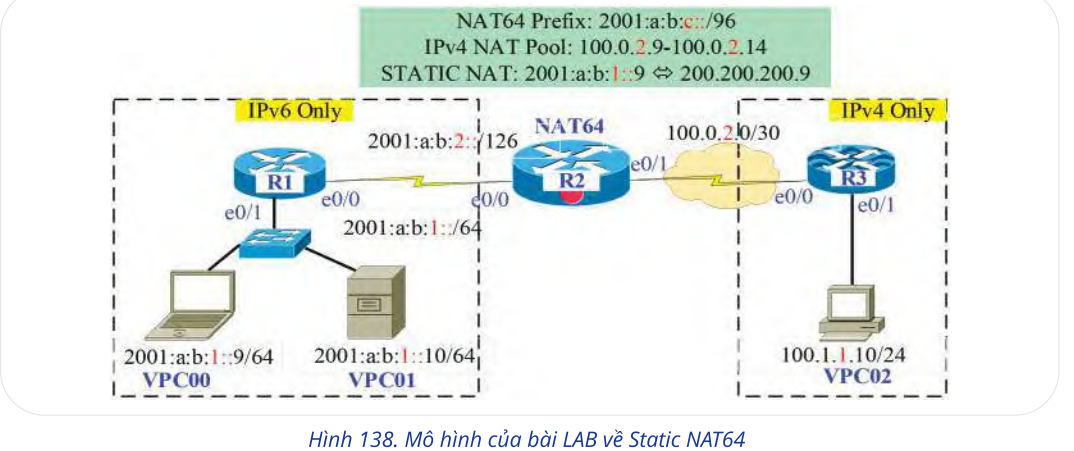
Tiến hành Ping, Trace thêm từ R1 và VPC01 đến VPC02, chúng ta thấy kết quả sau:

```
R2#show nat64 translations
Proto       Original IPv4        Translated IPv4
            Translated IPv6      Original IPv6
---------------------------------------------------------
udp         100.0.1.10:20657     [2001:A:B:C::6400:10A]:20657
            100.0.2.14:20656     [2001:A:B:1::10]:20656
udp         100.0.1.10:33470     [2001:A:B:C::6400:10A]:33470
            100.0.2.14:49194     [2001:A:B:2::1]:49194
```

Như vậy các địa chỉ IPv6 2001:A:B:1::10 và 2001:A:B:2::1 cùng được NAT64 chung địa chỉ 100.0.2.14. Trong bài LAB này, do số lượng kết nối giả lập ít nên địa chỉ Port không thay đổi. Nếu số lượng phiên kết nối tăng thì sẽ thấy các địa chỉ Port sẽ thay đổi khi dùng NAT64 Overload.

9.6. LAB03 – SỬ DỤNG STATIC NAT64 CHO INBOUND NAT

Hai bài LAB trên tập trung vào việc thiết lập kết nối từ các máy tính IPv6 Only đến các máy tính IPv4 Only bên ngoài. Tuy nhiên, để đáp ứng trường hợp các máy tính IPv4 Only cần truy cập các dịch vụ trên hệ thống mạng IPv6 Only thì chúng ta cần cấu hình **Static NAT64**. Trong cấu hình này, mỗi máy tính IPv6 Only sẽ được ánh xạ cố định với một địa chỉ IPv4 cụ thể. Có một điều đáng chú ý là cả **Dynamic NAT64** và **Static NAT64** có thể hoạt động đồng thời trên cùng một hệ thống, hỗ trợ linh hoạt cho nhu cầu sử dụng thực tế.



Hình 138. Mô hình của bài LAB về Static NAT64

Trong bài LAB Static NAT64 chúng ta sẽ thêm máy tính VPC00 có địa chỉ 2001:a:b:1::9/64, địa chỉ này sẽ được ánh xạ tĩnh với địa chỉ IPv4 200.200.200.9. Chú ý, địa chỉ IPv4 dùng cho Static NAT64 không được nằm trong POOLv4 dành cho Dynamic Nat64. Dưới đây là cấu hình bổ sung Static NAT64, các cấu hình của Dynamic NAT64 trong bài LAB trước vẫn được giữ lại cho các phiên kết nối từ IPv6 sang IPv4.

```
R2#show running-config | include static
nat64 v6v4 static 2001:A:B:1::9 200.200.200.9
R2#
```

Thực hiện Ping từ VPC02 từ mạng IPv4 sang VPC00 của mạng IPv6, kết quả thành công.

```
VPC02> ping 200.200.200.9

84 bytes from 200.200.200.9 icmp_seq=1 ttl=58 time=4.645 ms
84 bytes from 200.200.200.9 icmp_seq=2 ttl=58 time=5.487 ms
84 bytes from 200.200.200.9 icmp_seq=3 ttl=58 time=5.719 ms
84 bytes from 200.200.200.9 icmp_seq=4 ttl=58 time=7.911 ms
84 bytes from 200.200.200.9 icmp_seq=5 ttl=58 time=16.313 ms
```

Thực hiện Ping từ VPC01 từ mạng IPv6 sang VPC02 của mạng IPv4, kết quả thành công. Như vậy các kết nối xuất phát từ mạng IPv4 hoặc IPv6 đều hoạt động, có nghĩa Dynamic và Static NAT64 có thể hoạt động đồng thời.

```
VPC01> ping 2001:a:b:c::100.0.1.10

2001:a:b:c::100.0.1.10 icmp6_seq=1 ttl=61 time=16.038 ms
2001:a:b:c::100.0.1.10 icmp6_seq=2 ttl=61 time=7.094 ms
2001:a:b:c::100.0.1.10 icmp6_seq=3 ttl=61 time=4.938 ms
2001:a:b:c::100.0.1.10 icmp6_seq=4 ttl=61 time=5.897 ms
2001:a:b:c::100.0.1.10 icmp6_seq=5 ttl=61 time=4.009 ms
```

Kiểm tra trạng thái hoạt động của NAT64 trên R2 chúng ta thấy rõ việc ánh xạ cho Static và Dynamic NAT64.

```
R2#show nat64 translations
Proto      Original IPv4     Translated IPv4
           Translated IPv6   Original IPv6
------------------------------------------------------------
icmp       100.0.1.10:11606  [2001:A:B:C::6400:10A]:11606
           200.200.200.9:11606[2001:A:B:1::9]:11606
---------
           200.200.200.9     2001:A:B:1::9       Static NAT64

icmp       100.0.1.10:12374  [2001:A:B:C::6400:10A]:12374
           100.0.2.10:12374  [2001:A:B:1::10]:12374
---------
           100.0.2.10        2001:A:B:1::10     Dynamic NAT64
```

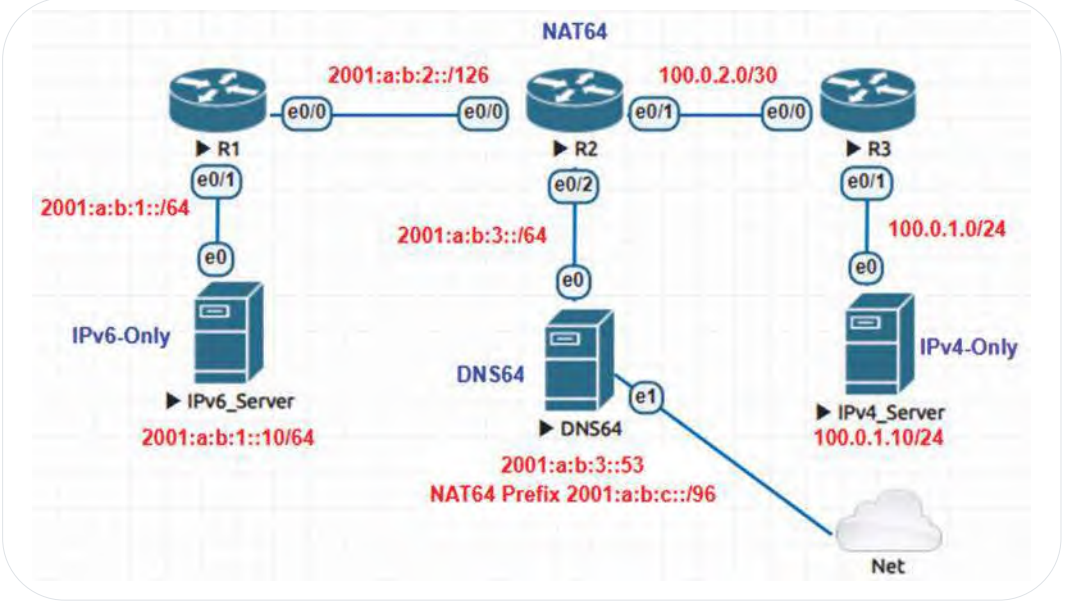
9.7. LAB04 – SỬ DỤNG DNS64 SERVER CHẾ ĐỘ IPv6 ONLY LÀM RESOLVER CHO KẾT NỐI OUTBOUND

DNS64 đóng vai trò quan trọng khi kết hợp với NAT64, tạo thành một giải pháp hiệu quả để triển khai mạng IPv6 Only, đảm bảo khả năng kết nối liền mạch với mạng IPv4. Không chỉ thực hiện nhiệm vụ phân giải tên miền, DNS64 còn tự động chuyển đổi địa chỉ IPv4 từ kết quả phân giải tên miền thành địa chỉ IPv6 thông qua kết hợp với NAT64 Prefix. Nhờ đó, các thiết bị IPv6 Only có thể truy cập các thiết bị IPv4 Only thông qua tên miền được phân giải bởi DNS64.

Trong bài LAB này, chúng ta sử dụng phần mềm BIND để cài đặt và cấu hình DNS64 Server. BIND là một phần mềm DNS Server nổi tiếng và được sử dụng rộng rãi trên toàn thế giới nhờ tính linh hoạt, mạnh mẽ và độ tin cậy cao. Là phần mềm mã nguồn mở, BIND không chỉ giúp tiết kiệm chi phí cho doanh nghiệp mà còn cho phép tùy chỉnh theo nhu cầu cụ thể.

Một ưu điểm lớn của BIND là hỗ trợ đầy đủ các tính năng tiên tiến như DNS64, DNSSEC và quản lý vùng (zone management), giúp đảm bảo hiệu năng và tính bảo mật của hệ thống DNS. Bên cạnh đó, BIND được cộng đồng phát triển và hỗ trợ mạnh mẽ, cung cấp các bản cập nhật thường xuyên để khắc phục lỗi và tăng cường bảo mật. Sử dụng BIND làm DNS64 Server trong bài LAB không chỉ minh họa khả năng triển khai một cách hiệu quả mà còn thể hiện lợi ích trong việc áp dụng giải pháp mã nguồn mở cho hệ thống mạng IPv6 Only.

Mô hình LAB chỉ có một chút thay đổi là thay các VPC thành các máy tính Ubuntu chạy IPv6 Only và IPv4 Only. Máy chủ DNS64 trong bài LAB này cũng chỉ sử dụng IPv6 Only với địa chỉ 2001:a:b:3::53. NAT64 Prefix vẫn giữ nguyên như các bài LAB trước là 2001:a:b:c::/96.



Hình 139. Mô hình của bài LAB sử dụng IPv6 Only DNS64

Dưới đây là các bước cài đặt và cấu hình cho BIND, DNS64 và Domain www.ipv4only.com trỏ tới địa chỉ 100.0.1.10. Cuối cùng thực hiện kiểm tra hoạt động của DNS64 và NAT64 thông qua kiểm tra kết nối từ máy tính IPv6 Only đến tên miền www.ipv4only.com.

BƯỚC 1: CÀI ĐẶT BIND

Đầu tiên cần cập nhật cho Ubuntu và cài đặt phần mềm BIND9 qua các lệnh sau:

```
sudo apt update
sudo apt install bind9 bind9utils bind9-doc
```

BƯỚC 2: CẤU HÌNH BIND CHO DNS64

Thực hiện mở file named.conf.options để cấu hình cho DNS64 thông qua lệnh:

```
sudo nano /etc/bind/named.conf.options
```

Các nội dung khai báo như trong hình sau:

```
        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bi
        //========================================================================
        dnssec-validation no;

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
        dns64 2001:a:b:c::/96 {
                clients { any; };
        };
        recursion no;
};

user@binhnv_ubuntu:/etc/bind$
```

Hình 140. Khai báo cho named.conf.options

Trong bài LAB này chúng ta tạm bỏ qua tính năng DNSSec vì có thể gây xung đột với NAT64. Phần quan trọng nhất là khai báo NAT64 Prefix cho DNS64 vì DNS64 sẽ gán Prefix này nếu kết quả phân giải tên miền là địa chỉ IPv4. Ngoài ra khai báo thêm cho phép không giới hạn các DNS Client và Recursion là No để việc kiểm tra hoạt động của NAT64 chỉ trong phạm vi của bài LAB, không làm chậm việc kiểm tra về sau.

BƯỚC 3: CẤU HÌNH ZONE CHO TÊN MIỀN IPV4ONLY.COM

Thực hiện mở file named.conf.local để cấu hình tên miền mới thông qua lệnh:

```
sudo nano /etc/bind/named.conf.local
```

Nội dung cần khai báo như sau:

```
zone "ipv4only.com" {
        type master;
        file "/etc/bind/db.ipv4only.com";
};
```

Hình 141. Khai báo cho named.conf.local

Trong hình này, ipv4only.com là tên miền cần khai báo, sẽ trỏ đến địa chỉ của máy tính thuộc miền IPv4 là 100.0.1.10. Thông tin liên quan khai báo cho tên miền này được lưu trong file db.ipv4only.com sẽ được trình bày tiếp theo sau. Tiếp tục sửa file thông tin bằng lệnh:

```
sudo nano /etc/bind/db.ipv4only.com
```

Nội dung sẽ sửa đổi theo quy hoạch của bài LAB như bên dưới.

```
user@binhnv_ubuntu:~$ cat /etc/bind/db.ipv4only.com
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns1.ipv4only.com. admin.ipv4only.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns1.ipv4only.com.
ns1     IN      AAAA    2001:a:b:3::53
www     IN      A       100.0.1.10
```

Hình 142. Khai báo cho db.ipv4only.com

Chúng ta có thể thấy địa chỉ của Name Server là địa chỉ IPv6 2001:a:b:3::53 còn địa chỉ tên miền www.ipv4only.com lại là địa chỉ IPv4 100.0.1.10.

BƯỚC 4: KIỂM TRA KHAI BÁO VÀ KHỞI ĐỘNG LẠI BIND

Để chắc chắn các khai báo đã đúng theo yêu cầu và đúng cấu trúc, chúng ta dùng các lệnh kiểm tra sau:

```
sudo named-checkconf
sudo named-checkzone ipv4only.com /etc/bind/db. ipv4only.com
```

Các lệnh trên kiểm tra khai báo trong các File named.conf.options, named.conf.local và db.ipv4only.com.
Dùng lệnh sau để khởi động lại dịch vụ BIND và kiểm tra trạng thái hoạt động của BIND sau khi khởi động lại.

```
sudo systemctl restart bind9
sudo systemctl status bind9
```

9.8. LAB05 – KIỂM TRA HOẠT ĐỘNG CỦA DNS64 VÀ NAT64 CHO KẾT NỐI OUTBOUND

Sau khi cấu hình NAT64 và DNS64 trong các bài LAB trên chúng ta tiến hành kiểm tra hoạt động của giải pháp kết hợp này. Trong bài LAB này, chúng ta sử dụng máy tính Ubuntu thuộc mạng IPv6, có địa chỉ 2001:a:b:1::10 để kiểm tra kết nối đến tên miền www.ipv6only.com.

Đầu tiên chúng ta khai báo địa chỉ IPv6 tĩnh cho máy tính Ubuntu, điều này có thể không cần thiết vì máy tính có thể tự gán IPv6 động theo cơ chế SLAAC nhưng đây cũng là cách chúng ta làm quen lệnh khai báo cho Ubuntu. Ngoài ra cũng cần đặt địa chỉ DNS Server là địa chỉ của máy chủ DNS64.

```
File  Edit  View  Search  Terminal  Help
user@ipv6_server:~$ cat /etc/netplan/01-network-manager-all.yaml
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      dhcp6: no
      addresses:
        - 2001:a:b:1::10/64
      gateway6: 2001:a:b:1::1
      nameservers:
        addresses:
          - 2001:a:b:3::53
```

Hình 143. Kiểm tra khai báo cho Netplan

Để việc phân giải tên miền nhanh hơn thì chúng ta nên khai báo địa chỉ DNS Server trong File /etc/resolv.conf như hình dưới.

```
nameserver 2001:a:b:3::53
options edns0

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text
```

Hình 144. Khai báo nameserver cho /etc/resolv.conf

Chú ý:

- Thông thường, việc khai báo trong resolv.conf sẽ bị trả về mặc định là 127.0.0.53 sau khi máy tính Reboot. Các bạn cần tham khảo thêm trên Internet cách thức để cố định thông tin khai báo này.

Trên máy tính IPv6 Only thực hiện lệnh PING đến www.ipv4only.com, kết quả trả về là địa chỉ 2001:a:b:c::6400:10a. Địa chỉ này là địa chỉ kết hợp giữa NAT64 Prefix 2001:a:b:c::/96 đã khai báo trên NAT64 Router và tại DNS64 Server kết hợp giá trị Hexa của địa chỉ IPv4 100.0.1.10 đã khai cho địa chỉ www.ipv4only.com trên DNS64 Server.

```
user@ipv6_server:~$ ping www.ipv4only.com
PING www.ipv4only.com(2001:a:b:c::6400:10a (2001:a:b:c::6400:10a)) 56 data bytes
64 bytes from 2001:a:b:c::6400:10a (2001:a:b:c::6400:10a): icmp_seq=1 ttl=61 tim
e=28.9 ms
64 bytes from 2001:a:b:c::6400:10a (2001:a:b:c::6400:10a): icmp_seq=2 ttl=61 tim
e=3.79 ms
64 bytes from 2001:a:b:c::6400:10a (2001:a:b:c::6400:10a): icmp_seq=3 ttl=61 tim
e=7.55 ms
64 bytes from 2001:a:b:c::6400:10a (2001:a:b:c::6400:10a): icmp_seq=4 ttl=61 tim
e=3.68 ms
^C
--- www.ipv4only.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 3.681/10.986/28.917/10.469 ms
```

Hình 145. Thực hiện lệnh PING đến máy tính IPv4 Only

Kiểm tra trên NAT64 Router chúng ta thấy thông tin NAT giữa các địa chỉ IPv4 và IPv6.

```
R2#show nat64 translations
Proto          Original IPv4       Translated IPv4
               Translated          IPv6Original IPv6
------------------------------------------------------------
Icmp           100.0.1.10:2047     [2001:A:B:C::6400:10A]:2047
               100.0.2.10:2047     [2001:A:B:1::10]:2047
---------
               100.0.2.102001:A:B:1::10

Total number of translations: 2
```

Như vậy với sự kết hợp của DNS64 và NAT64 chúng ta thấy mạng IPv6 Only có thể truy cập trong suốt với mạng IPv4 Only. Trong đó, NAT64 có nhiệm vụ chuyển đổi giữa hai giao thức còn DNS64 giúp phân giải và chuyển đổi địa chỉ đích IPv4 thành IPv6 thông qua sự kết hợp với NAT64 Prefix được khai báo trên NAT64 Router. Có thể nói đây là giải pháp đơn giản, hiệu quả và tối ưu nhất để chuyển đổi mạng của các doanh nghiệp và trung tâm dữ liệu sang môi trường mạng IPv6 Only, nhằm đảm bảo tính ổn định và khả năng phát triển lâu dài trong kỷ nguyên IPv6..

Mặc dù vậy, DNS64/NAT64 cũng có hạn chế đối với các ứng dụng sử dụng trực tiếp địa chỉ IPv4 thay cho tên miền vì lúc đó DNS64 không thể can thiệp để chuyển đổi sang địa chỉ IPv6.

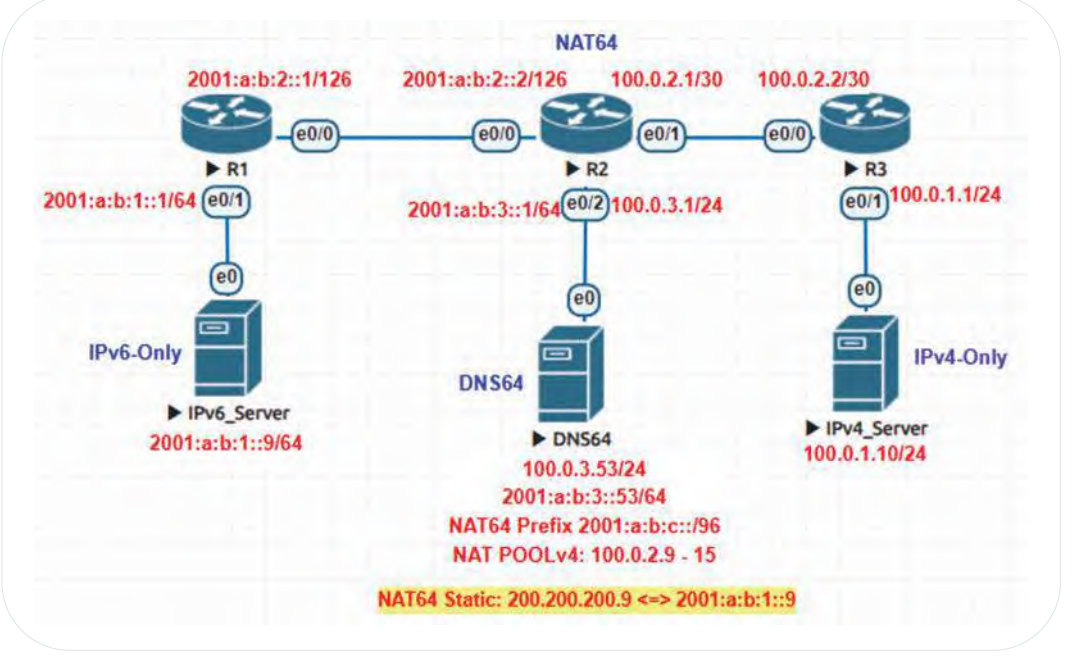
Một giải pháp có thể khắc phục hạn chế của DNS64/NAT64 là 464XLAT nhưng một số hệ điều hành như Windows không hỗ trợ tính năng CLAT (Customer-Side Translator) là một thành phần của 464XLAT. Vì thế không thể áp dụng giải pháp 464XLAT cho môi trường mạng doanh nghiệp và trung tâm dữ liệu.

9.9. LAB06 - SỬ DỤNG DNS64 CHẾ ĐỘ DUAL STACK LÀM AUTHORITATIVE SERVER CHO KẾT NỐI INBOUND

Các mô hình trên chúng ta sử dụng IPv6 Only DNS64 và tập trung cho cho hướng kết nối từ mạng IPv6 đến mạng IPv4. Tuy nhiêu trong thực tế, chúng ta gặp phải trường hợp các máy tính IPv6 bên trong cần cung cấp dịch vụ cho các các máy tính IPv4 bên ngoài truy cập vào. Lúc này chúng ta cần cấu hình một máy chủ Authoritative DNS Server. Trong LAB này, chúng ta sẽ tận dụng chính máy chủ DNS64 để đảm nhận vai trò Authoritative DNS Server. Cách đơn giản nhất là chúng ta sẽ thiết lập chế độ Dual Stack cho máy chủ DNS64.

Dưới đây là sơ đồ LAB và các thông tin chi tiết:

- **Máy chủ web IPv6:** Có tên miền là www.ipv6only.com và địa chỉ 2001:a:b:1::9/64.
- **NAT64 Static:** Địa chỉ IPv6 2001:a:b:1::9 được ánh xạ tĩnh thành địa chỉ IPv4 200.200.200.9. Cấu hình này đã được đề cập trong mô hình Static NAT64 ở phần trước.
- **Máy chủ web IPv4:** Có tên miền www.ipv4only.com và địa chỉ IPv4 100.0.1.10.
- **NAT64 Prefix:** Địa chỉ IPv4 100.0.1.10 sẽ được ánh xạ thành địa chỉ IPv6 thông qua tiền tố NAT64 2001:a:b:c::/96, cụ thể là 2001:a:b:c::6400:10a.
- **DNS64 Server:** Hoạt động ở chế độ Dual Stack với hai địa chỉ 100.0.3.53 (IPv4) và 2001:a:b:3::9 (IPv6). Các máy chủ IPv4 và IPv6 sẽ sử dụng các địa chỉ này làm DNS Server để kiểm tra kết quả."



Hình 146. Mô hình của bài LAB sử dụng Dual Stack DNS64

Phần cấu hình Static NAT64 cho R2 đã được trình bày ở trên nên sẽ không trình bày lại ở đây. Dưới đây là các nội dung cấu hình cho Dual Stack DNS64 Server.

BƯỚC 1: CẤU HÌNH ĐỊA CHỈ CHO DNS64 SERVER

Máy chủ DNS64 trong mô hình này hoạt động ở chế độ Dual Stack nên chúng ta cần cấu hình thông qua lệnh sau:

```
sudo nano /etc/netplan/01-network-manager-all.yaml
```

Thực hiện khai báo thông tin địa chỉ IPv4 và IPv6 như hình dưới.

```
File  Edit  View  Search  Terminal  Help
  GNU nano 2.9.3                  /etc/netplan/01-network-manager-all.yaml

# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      dhcp4: no
      dhcp6: no
      addresses:
        - 2001:a:b:3::53/64
        - 100.0.3.53/24
      gateway4: 100.0.3.1
      gateway6: 2001:a:b:3::1
      nameservers:
        addresses:
          - 2001:a:b:3::53
```

Hình 147. Khai báo cho Netplan

BƯỚC 2: CẤU HÌNH THÔNG TIN CÁC ZONE LIÊN QUAN

Việc cấu hình cho NAT64 Prefix cho DNS64 thực hiện giống như các bài LAB ở trên. Ở đây chúng ta bổ sung khai báo Zone tương ứng tên miền www.ipv4only và www.ipv6only.com, gồm cả tên miền thuận và ngược. thông qua sửa đổi file named.conf.local.

```
sudo nano /etc/bind/named.conf.local
```

Các thông tin khai báo như bên dưới.

```
user@binhnv_ubuntu:/etc/bind$ cat named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used i
// organization
//include "/etc/bind/zones.rfc1918";

zone "ipv4only.com" {
        type master;
        file "/etc/bind/db.ipv4only.com";
};

zone "ipv6only.com" {
        type master;
        file "/etc/bind/db.ipv6only.com";
};

// Reverse zone cho www.ipv4only.com
zone "1.0.100.in-addr.arpa" {
        type master;
        file "etc/bind/db.1.0.100.rev";
};
// Reverse zone cho www.ipv6only.com voi IPv4 200.200.200.9
zone "200.200.200.in-addr.arpa" {
        type master;
        file "/etc/bind/db.200.200.200.rev";
};
// Reverse zone cho www.ipv4only.com voi IPv6 2001:a:b:1::9
zone "1.0.0.0.b.0.0.0.a.0.0.0.1.0.0.2.ip6.arpa" {
        type master;
        file "/etc/bind/db.ipv6only.rev";
};
```

Hình 148. Khai báo cho named.conf.local

Trong File này chúng ta khai báo Zone thuận cho ipv4only.com và ipv6only.com và Zone ngược cho ipv4only.com. Đối với Zone ngược cho ipv6only.com thì chúng ta cần khai Zone ngược cho địa chỉ IPv4 (200.200.200.9) và cho địa chỉ IPv6 (2001:a:b:1::9). Với Zone ngược cho ipv6only.com thì chúng ta chỉ khai tên Zone gồm 16 Nibble (mỗi Nibble gồm 4 bit, tương tương 1 số Hexa) của địa chỉ IPv6 (2001:a:b:1::9/64) và đảo ngược lại vị trí. Chú ý không được bỏ các số 0 bị thu gọn mà phải viết đầy đủ.

BƯỚC 3: CẤU HÌNH CÁC FILE ZONE LIÊN QUAN

Tiếp theo chúng ta khai thông tin chi tiết cho các Zone đã khai báo ở trên tương ứng với thông tin địa chỉ IPv4, IPv6 đã quy hoạch theo sơ đồ LAB, khai báo tên miền thuận và tên miền miền ngược cho các Zone.

Khai báo cho tên miền thuận: db.ipv4only.com

```
user@binhnv_ubuntu:/etc/bind$ cat db.ipv4dnly.com
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns1.ipv4only.com. admin.ipv4only.com. (
                              11         ; Serial
                          604800         ; Refresh
                           86400         ; Retry
                         2419200         ; Expire
                          604800 )       ; Negative Cache TTL
;
@       IN      NS      ns1.ipv4only.com.
@       IN      A       100.0.1.10
ns1     IN      A       100.0.3.53
ns1     IN      AAAA    2001:a:b:3::53
www     IN      A       100.0.1.10
```

Hình 149. Khai báo cho Zone ipv4only.com

Khai báo cho tền miền thuân: db.ipv6only.com

```
user@binhnv_ubuntu:/etc/bind$ cat db.ipv6only.com
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns1.ipv6only.com. admin.ipv6only.com. (
                           20240203       ; Serial
                          604800          ; Refresh
                           86400          ; Retry
                         2419200          ; Expire
                          604800 )        ; Negative Cache TTL
;
@       IN      NS      ns1.ipv6only.com.
@       IN      A       200.200.200.9
@       IN      AAAA    2001:a:b:1::9
;
ns1     IN      A       100.0.3.53
;
www     IN      A       200.200.200.9
www     IN      AAAA    2001:a:b:1::9
```

Hình 150. Khai báo cho Zone ipv6only.com

Khai báo cho tên miền ngược: db.1.0.100.rev

```
user@binhnv_ubuntu:/etc/bind$ cat db.1.0.100.rev
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns1.ipv4only.com. admin.ipv4only.com.
                        20250203        ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL

        IN      NS      ns1.ipv4only.com.
10      IN      PTR     www.ipv4only.com.
```

Hình 151. Khai báo cho Zone ngược ipv4only.com

Khai báo cho tên miền ngược: db.ipv6only.rev

```
user@binhnv_ubuntu:/etc/bind$ cat db.ipv6only.rev
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL    86400
@       IN      SOA     ns1.ipv4only.com. admin.ipv4only.com. (
                         20250207       ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL

        IN      NS      ns1.ipv4only.com.

;Khai bao ban ghi PTR cho dia chi IPv6
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0  IN PTR www.ipv6only.com.
```

Hình 152. Khai báo cho Zone ngược ipv6only.com

Trong File named.conf.local chúng ta đã khai báo Zone ngược cho địa chỉ IPv6 của Domain ipv6only.com gồm 64 bit đầu tiên của địa chỉ IPv6. Ở đây chúng ta chỉ cần khai báo 64 bit còn lại của địa chỉ IPv6 nhưng được viết ngược lại sau khi chuyển đổi ra số Hexa đầy đủ.

BƯỚC 4: KIỂM TRA PHÂN GIẢI THUẬN

Đầu tiên kiểm tra kết nối từ máy tính thuộc phân vùng IPv6 đến tên miền www.ipv4only.com thuộc vùng IPv4.

```
user@ipv6_server:~$ ping www.ipv4only.com
PING www.ipv4only.com(2001:a:b:c::6400:10a (2001:a:b:c::6400:10a)) 56 data bytes
64 bytes from 2001:a:b:c::6400:10a (2001:a:b:c::6400:10a): icmp_seq=1 ttl=61 tim
e=15.2 ms
64 bytes from 2001:a:b:c::6400:10a (2001:a:b:c::6400:10a): icmp_seq=2 ttl=61 tim
e=6.30 ms
64 bytes from 2001:a:b:c::6400:10a (2001:a:b:c::6400:10a): icmp_seq=3 ttl=61 tim
e=3.72 ms
64 bytes from 2001:a:b:c::6400:10a (2001:a:b:c::6400:10a): icmp_seq=4 ttl=61 tim
e=2.95 ms
^C
--- www.ipv4only.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3032ms
rtt min/avg/max/mdev = 2.952/7.049/15.219/4.877 ms
```

Hình 153. Thực hiện PING kiểm tra máy tính IPv4 Only từ máy tính IPv6 Only

Kết quả PING trả về địa chỉ 2001:a:b:c::6400:10a, đây là địa chỉ kết hợp từ NAT64 Prefix với địa chỉ IPv4 100.0.1.10 (6400:10a).

Tiếp theo thực hiện kiểm tra phân giải từ máy tính thuộc vùng IPv4 đến địa chỉ www.ipv6only.com thuộc vùng IPv6.

```
user@ipv4_server:~$ ping www.ipv6only.com
PING www.ipv6only.com (200.200.200.9) 56(84) bytes of data.
64 bytes from www.ipv6only.com (200.200.200.9): icmp_seq=1 ttl=61 time=4.91 ms
64 bytes from www.ipv6only.com (200.200.200.9): icmp_seq=2 ttl=61 time=8.50 ms
64 bytes from www.ipv6only.com (200.200.200.9): icmp_seq=3 ttl=61 time=25.3 ms
64 bytes from www.ipv6only.com (200.200.200.9): icmp_seq=4 ttl=61 time=5.29 ms
^C
--- www.ipv6only.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 4.912/11.021/25.374/8.403 ms
```

Hình 154. Thực hiện PING kiểm tra máy tính IPv6 Only từ máy tính IPv4 Only

Kết quả PING cho thấy địa chỉ trả về là địa chỉ IPv4 200.200.200.9, đây là địa chỉ được ánh xạ tĩnh (Static NAT64) của địa chỉ IPv6 2001:a:b:1::9. Điều này khẳng định hoạt động của DNS64 và NAT64 là đúng như mong muốn.

BƯỚC 5: KIỂM TRA PHÂN GIẢI NGƯỢC

Đầu tiên thực hiện lệnh DIG nhằm kiểm tra phân giải tên miền ngược từ máy tính IPv6 đối với địa chỉ 2001:a:b:1::9 cho tên miền www.ipv6only.com, kết quả dưới đây cho thấy việc khai báo và phân giải như yêu cầu.

```
user@ipv6_server:~$ dig -x 2001:a:b:1::9

; <<>> DiG 9.11.3-1ubuntu1.15-Ubuntu <<>> -x 2001:a:b:1::9
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7999
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.b.0.0.0.a.0.0.0.1.0.0.2.ip6.arpa. IN PT
R

;; ANSWER SECTION:
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.b.0.0.0.a.0.0.0.1.0.0.2.ip6.arpa. 86400I
N PTR www.ipv6only.com.

;; Query time: 7 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Feb 07 02:25:37 GMT 2025
;; MSG SIZE  rcvd: 131
```

Hình 155. Kiểm tra phân giải ngược cho địa chỉ IPv6

Tương tự, chúng ta thực hiện phân giải ngược từ máy tính IPv4.

```
user@ipv4_server:~$ dig -x 200.200.200.9

; <<>> DiG 9.11.3-1ubuntu1.15-Ubuntu <<>> -x 200.200.200.9
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34653
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;9.200.200.200.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
9.200.200.200.in-addr.arpa. 604800 IN   PTR     www.ipv6only.com.

;; Query time: 31 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Feb 07 02:30:45 GMT 2025
;; MSG SIZE  rcvd: 85
```

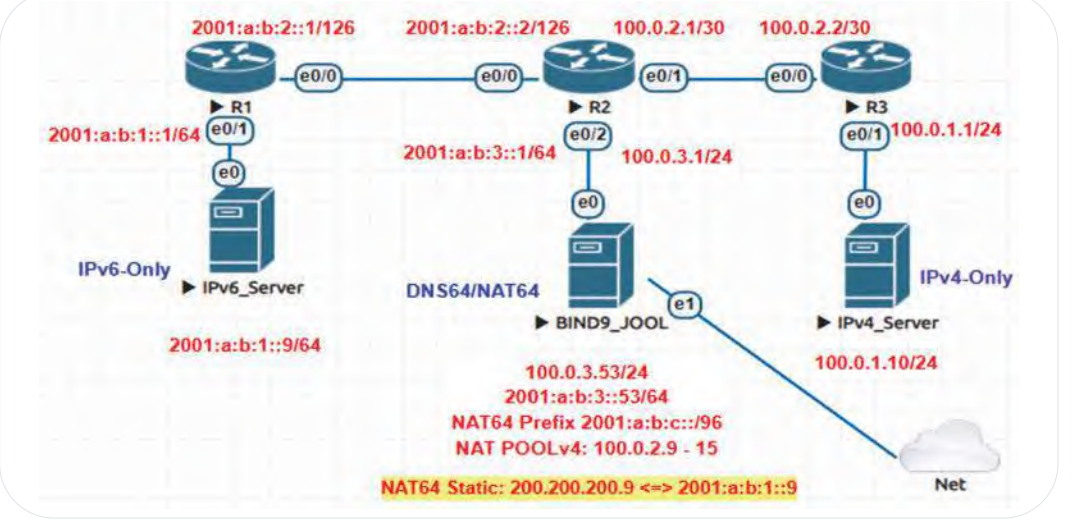
Hình 156. Kiểm tra phân giải ngược cho địa chỉ IPv4

Kết quả lệnh DIG trả về địa chỉ IPv4 200.200.200.9 là địa chỉ NAT64 của 2001:a:b:1::9, như vậy nội dung khai báo đã hoạt động tốt.

Trên đây là toàn bộ khai báo và các bước kiểm tra cho mô hình sử dụng NAT64 và DN64, trong đó máy chủ DNS64 là Authoraitative DNS cho cả hai tên miền và hoạt động ở chế độ Dual Stack. Các bước kiểm tra cho thấy việc phân giải tên miền thuận và ngược đều hoạt động tốt. Đây là mô hình có thể đáp ứng nhu cầu thực tiễn trong đó các máy tính vùng IPv4 có thể kết nối liền mạch với máy tính IPv4, đồng thời cho phép các máy tính IPv4 truy cập các máy chủ thuộc vùng IPv6.

9.10. LAB07 – MÔ HÌNH TÍCH HỢP DNS64/NAT64

Đây là mô hình ứng dụng trong tình huống các cơ quan, doanh nghiệp, tổ chức không có thiết bị router hỗ trợ NAT64. Trong mô hình này, tính năng NAT64 và DNS64 cùng tích hợp trên một máy tính, không cần sự can thiệp của thiết bị router bên ngoài.



Hình 157. Mô hình của bài LAB IPv6 Only tích hợp giữa NAT64 và DNS64

Đây là mô hình để thực hiện LAB, bao gồm 3 thiết bị router, 3 máy tính Ubuntu. Các thiết bị router chỉ đóng vai trò kết nối, không tham gia trực tiếp vào việc NAT64. R2 hoạt động ở chế độ IPv6 Only với phân vùng bên trái và IPv4 với phân vùng IPv4 Only. Máy chủ DNS64/NAT64 hoạt động chế độ Dual Stack. Thực tế chúng ta có thể dùng máy chủ DNS64/NAT64 làm Gateway cho cả phân vùng IPv6 và IPv4, thay cho R2. Điểm thuận tiện của mô hình LAB này cho phép triển khai IPv6 Only từng bước mà không phải thay đổi nhiều cùng một lúc, làm ảnh hưởng hoạt động hệ thống hiện tại.

Ngoài BIND9 được sử dụng cho tính năng DNS64 thì ở bài LAB này chúng ta sẽ sử dụng phần mềm Jool cho tính năng NAT64. Jool là phần mềm mã nguồn mở chạy trên nền Linux giúp kết nối giữa mạng IPv6 Only và IPv4 Only mà không cần phải thay đổi hạ tầng. Jool hỗ trợ cả NAT64 (dịch địa chỉ động) và SIIT (dịch địa chỉ 1:1), giúp chúng ta triển khai hệ thống linh hoạt, đơn giản và chi phí thấp.

Trong bài LAB này chúng ta chỉ thực hiện sử dụng Jool để thực hiện NAT64 nhằm hỗ trợ các máy tính IPv6 có thể truy cập các máy tính IPv4. Giải pháp này phù hợp với các hệ thống có quy mô nhỏ và vừa. Đối với hệ thống lớn như Datacenter, cho phép truy cập từ bên ngoài mạng IPv4 vào mạng IPv6 thì chúng ta nên triển khai các thiết bị Router, Firewall chuyên dụng có hỗ trợ Static NAT64 như trong các bài LAB trình bày trước.

Chú ý:
- Server BIND9/JOOL khai Default Gateway IPv4 và IPv6 về router.
- Router thêm Route đến Prefix 2001:a:b:c::/96 trỏ về Server BIND9/JOOL.

Nội dung bài LAB bao gồm các bước cài đặt và cấu hình Bind9 và Jool để cho phép các máy tính IPv6 có thể truy cập được tên miền www.ipv4only có địa chỉ IPv4 là 100.0.1.10, sử dụng NAT64 Prefix là 2001:a:b:c::/96. Các địa chỉ IPv4 và IPv6 được quy hoạch trong sơ đồ trên.

Bước 1: Cài đặt và cấu hình Bind9 để làm DNS64 Server

Việc khai báo máy chủ DNS64 như các ví dụ trên. Ở đây để đơn giản hóa chỉ thực hiện tên miền thuận cho www.ipv4only.com. Dưới đây là một số thông tin về khai báo cho Bind9.

```
==
        dnssec-validation no;

        auth-nxdomain no;    # conform to RFC1035
        dns64 2001:a:b:c::/96 {
                clients {any;};
        };
        listen-on-v6 { any; };
};

user@bind9_jool:~$
```

```
user@bind9_jool:~$ cat /etc/bind/named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not
// organization
//include "/etc/bind/zones.rfc1918";

zone "ipv4only.com" {
        type master;
        file "/etc/bind/db.ipv4only.com";
};
```

```
user@bind9_jool:~$ cat /etc/bind/db.ipv4only.com
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns1.ipv4only.com. admin.ipv4only.com. (
                              100         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns1.ipv4only.com.
@       IN      A       100.0.1.10
ns1     IN      A       100.0.3.10
www     IN      A       100.0.1.10
```

Hình 158. Các khai báo cho DNS64

Kiểm tra khai báo cho DNS64 từ máy tính IPv6 Only.

```
user@ipv6_server:~$ dig AAAA www.ipv4only.com

; <<>> DiG 9.11.3-1ubuntu1.15-Ubuntu <<>> AAAA www.ipv4only.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46072
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.ipv4only.com.              IN      AAAA

;; ANSWER SECTION:
www.ipv4only.com.       604800  IN      AAAA    2001:a:b:c::6400:10a
```

Hình 159. Kiểm tra kác khai báo cho DNS64

Bước 2: Cài đặt phần mềm Jool

Đầu tiên, nên thực hiện cập nhật hệ điều hành và các gói phần mềm liên quan thông qua các lệnh sau:

```
sudo apt-get update
sudo apt-get upgrade
sudo apt-get install -y build-essential dkms libnl-3-dev libnl-genl-3-dev pkg-
config iproute2 iptables
```

```
user@bind9_jool:~$ sudo apt-get install -y build-essential dkms libnl-3-dev libn
l-genl-3-dev pkg-config iproute2 iptables
```

Hình 160. Cập nhật các gói phần mềm trước khi cài đặt Jool

Tiếp theo tải các File cài đặt cho Jool và tiến hành cài đặt.

```
wget https://www.jool.mx/download/jool-dkms_4.1.7-1_all.deb
wget https://www.jool.mx/download/jool-tools_4.1.7-1_amd64.deb
sudo apt install ./ jool-dkms_4.1.7-1_all.deb ./jool-tools_4.1.7-1_amd64.deb
```

```
user@bind9_jool:~$ sudo apt install ./jool-dkms_4.1.7-1_all.deb  ./jool-tools_4.
1.7-1_amd64.deb
```

Hình 161. Tải và cài đặt phần mềm Jool

Tiếp theo thực hiện lệnh sau để kích hoạt Jool

```
sudo modprobe jool
```

Bước 3: Cấu hình NAT64 Prefix cho Jool

Để Jool thực hiện NAT64 thì cần khai báo NAT64 Prefix thông qua lệnh bên dưới, với "default" là tên gọi của một Instance trong Jool. Nên đặt tên "default" này cho Instance đầu tiên và gán NAT64 Prefix 2001:a:b:c::/96 theo quy hoạch.

```
sudo jool instance add 'default' --netfilter --pool6 2001:a:b:c::/96
```

Tiếp bật tính năng IP Forwarding cho IPv4 và IPv6 các cổng mạng trong Ubuntu.

```
sudo sysctl -w net.ipv6.conf.all.forwarding=1
sudo sysctl -w net.ipv6.conf.default.forwarding=1
sudo sysctl -w net.ipv4.ip_forward=1
sysctl -system
```

Bước 4: Kiểm tra hoạt động của Jool

Dùng các lệnh sau kiểm tra hoạt động của Jool.

```
Kiểm tra instace
jool instance display
jool instance status

Kiểm tra sessions
jool session display

Kiểm tra Global config
jool global display

Kiểm tra thông tin thống kê hoạt động
jool stats display

Kiểm tra trạng thái hoạt động của instance cụ thể
jool -i default instance status
```

```
user@bind9_jool:~$ jool instance display
+--------------------+------------------+-----------+
|          Namespace |             Name | Framework |
+--------------------+------------------+-----------+
|           aa7dd000 |          default | netfilter |
+--------------------+------------------+-----------+
user@bind9_jool:~$
user@bind9_jool:~$ jool global display
  manually-enabled: true
  pool6: 2001:a:b:c::/96
  lowest-ipv6-mtu: 1280
  logging-debug: false
```

Hình 162. Kiểm tra hoạt động của Jool sau khai báo

Bước 5: Kiểm tra hoạt động của DNS64 và NAT64

Trên máy tính IPv6 thực hiện lệnh PING đến địa chỉ www.ipv4only.com, chúng ta thấy tên miền được phân giải ra thành 2001:a:b:c::6400:10a và kết quả phản hồi thành công. Như vậy việc kết hợp giữa DNS64 bởi Bind9 và NAT64 bởi Jool có thể hoạt động tốt khi tích hợp cùng nhau trên cùng máy chủ Ubuntu.

```
user@ipv6_server:~$ ping -n www.ipv4only.com
PING www.ipv4only.com(2001:a:b:c::6400:10a) 56 data bytes
64 bytes from 2001:a:b:c::6400:10a: icmp_seq=1 ttl=125 time=326 ms
64 bytes from 2001:a:b:c::6400:10a: icmp_seq=2 ttl=125 time=248 ms
64 bytes from 2001:a:b:c::6400:10a: icmp_seq=3 ttl=125 time=242 ms
64 bytes from 2001:a:b:c::6400:10a: icmp_seq=4 ttl=125 time=254 ms
^C
--- www.ipv4only.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 242.302/267.967/326.564/34.101 ms
user@ipv6_server:~$
```

Hình 163. Kiểm tra hoạt động của Jool và Bind sau khi cấu hình

9.11. TỔNG KẾT CHƯƠNG 9

Chương 9 đã cung cấp cái nhìn tổng quan về mô hình mạng IPv6-Only và cách triển khai NAT64/DNS64 để duy trì kết nối giữa mạng IPv6 và các hệ thống chỉ hỗ trợ IPv4. Thông qua các bài thực hành, chương này hướng dẫn chi tiết các phương pháp NAT64, bao gồm Dynamic NAT64, Overload NAT64 và Static NAT64, đáp ứng nhu cầu kết nối Outbound và Inbound. Ngoài ra, các bài LAB còn mô tả việc cấu hình DNS64 ở chế độ Resolver và Authoritative Server, hỗ trợ hiệu quả cho quá trình chuyển đổi.

Việc triển khai IPv6 Only đánh dấu bước tiến quan trọng hướng tới hệ thống mạng toàn IPv6, tối ưu hóa tài nguyên địa chỉ và giảm sự phụ thuộc vào IPv4. Tuy nhiên, trong giai đoạn chuyển đổi, giải pháp NAT64/DNS64 đóng vai trò thiết yếu, đảm bảo khả năng tương thích ngược với các hệ thống IPv4, duy trì kết nối liền mạch và hiệu quả.

9.12. CÂU HỎI ÔN TẬP CHƯƠNG 9

01 **Tại sao nên chuyển đổi sang mô hình mạng IPv6 Only?**

Mô hình mạng IPv6 Only được xem là giải pháp chiến lược và bền vững do giải quyết triệt để vấn đề cạn kiệt địa chỉ IPv4 và loại bỏ sự phức tạp khi phải duy trì song song cả hai giao thức. Nó giúp đơn giản hóa hạ tầng, tối ưu hóa công tác vận hành và đáp ứng khả năng mở rộng trong tương lai, trở thành xu hướng được áp dụng rộng rãi.

02 **Thách thức lớn nhất khi triển khai IPv6 Only là gì và giải pháp nào được đề xuất?**

Thách thức lớn nhất là đảm bảo khả năng kết nối liên tục với các hệ thống, dịch vụ và ứng dụng vẫn hoạt động trên IPv4 Only. Để giải quyết vấn đề này, nhiều giải pháp đã được phát triển tùy thuộc vào loại hình mạng. Đối với mạng di động hoặc cố định quy mô lớn thường sử dụng 6RD, DS-Lite hoặc 464XLAT. Trong khi đó, đối với mạng doanh nghiệp và trung tâm dữ liệu, giải pháp dựa trên DNS64/NAT64 được ưa chuộng nhờ sự đơn giản, hiệu quả và thời gian triển khai nhanh chóng.

03 **NAT64 và DNS64 hoạt động như thế nào để hỗ trợ kết nối giữa mạng IPv6 Only và IPv4 Only?**

NAT64 (Network Address Translation from IPv6 to IPv4) cho phép các thiết bị trong mạng IPv6 Only giao tiếp với các dịch vụ và thiết bị IPv4 Only bằng cách dịch địa chỉ IPv6 thành địa chỉ IPv4 và ngược lại. DNS64 (DNS for IPv6) kết hợp với NAT64 bằng cách tự động chuyển đổi địa chỉ IPv4 từ kết quả phân giải tên miền thành địa chỉ IPv6 có tiền tố NAT64. Nhờ đó, các thiết bị IPv6 Only có thể truy cập các tài nguyên IPv4 Only thông qua tên miền.

04 **Có những mô hình triển khai NAT64/DNS64 nào được đề cập trong cuốn sách?**

Nội dung cuốn sách đề cập đến hai mô hình triển khai chính:

- Mô hình độc lập: Trong mô hình này, chức năng NAT64 và DNS64 hoạt động trên hai thiết bị riêng biệt. NAT64 thường được cấu hình trên router (nếu router hỗ trợ), còn DNS64 được triển khai trên một máy chủ độc lập.
- Mô hình tích hợp: Trong mô hình này, cả chức năng DNS64 và NAT64 được tích hợp trên cùng một máy chủ. Mô hình này phù hợp với các mạng không có router hỗ trợ NAT64 và có thể sử dụng các phần mềm mã nguồn mở như BIND cho DNS64 và Jool cho NAT64 trên hệ thống Linux.

05

Các loại hình NAT64 nào được trình bày và chúng khác nhau như thế nào?

Nội dung cuốn sách trình bày ba loại hình NAT64 chính:

- Dynamic NAT64: Ánh xạ địa chỉ IPv6 sang địa chỉ IPv4 theo kiểu 1:1 một cách động khi có kết nối được khởi tạo từ mạng IPv6.
- Overload NAT64 (tương tự PAT): Cho phép nhiều địa chỉ IPv6 chia sẻ một hoặc một vài địa chỉ IPv4 bằng cách sử dụng các cổng khác nhau, giúp tiết kiệm địa chỉ IPv4.
- Static NAT64: Ánh xạ cố định một địa chỉ IPv6 với một địa chỉ IPv4 cụ thể, thường được sử dụng khi các máy chủ IPv6 cần cung cấp dịch vụ cho người dùng IPv4.

06

BIND và Jool được sử dụng như thế nào trong việc triển khai IPv6 Only?

BIND (Berkeley Internet Name Domain) là một phần mềm DNS Server mã nguồn mở được sử dụng để triển khai chức năng DNS64. Nó có khả năng phân giải tên miền và tự động tổng hợp địa chỉ IPv6 từ địa chỉ IPv4 và tiền tố NAT64. Jool là một phần mềm mã nguồn mở chạy trên Linux, cung cấp khả năng NAT64, cho phép dịch địa chỉ giữa mạng IPv6 Only và IPv4 Only mà không cần thay đổi hạ tầng mạng.

07

Làm thế nào để một máy tính IPv6 Only có thể truy cập một máy tính IPv4 Only thông qua tên miền?

Quá trình này diễn ra như sau:

1. Máy tính IPv6 Only gửi yêu cầu phân giải tên miền (ví dụ: www.ipv4only.com) đến DNS64 Server.
2. DNS64 Server nhận thấy đây là tên miền trỏ đến địa chỉ IPv4 (ví dụ: 100.0.1.10).
3. DNS64 Server tổng hợp địa chỉ IPv6 bằng cách kết hợp tiền tố NAT64 (ví dụ: 2001:a:b:c::/96) với địa chỉ IPv4 (chuyển đổi hoặc nhúng vào tiền tố), tạo ra một địa chỉ IPv6 đích (ví dụ: 2001:a:b:c::6400:10a).
4. DNS64 Server trả về địa chỉ IPv6 đã tổng hợp cho máy tính IPv6 Only.
5. Máy tính IPv6 Only gửi gói tin đến địa chỉ IPv6 đã nhận.
6. Router hoặc máy chủ NAT64 nhận gói tin này và dịch địa chỉ IPv6 nguồn thành một địa chỉ IPv4 trong NAT Pool và địa chỉ IPv6 đích (đã chứa địa chỉ IPv4 nhúng) thành địa chỉ IPv4 đích ban đầu (100.0.1.10).
7. Gói tin sau khi được dịch sẽ được chuyển đến máy tính IPv4 Only. Quá trình ngược lại xảy ra khi máy tính IPv4 Only trả lời.

08

Giải pháp DNS64/NAT64 có những hạn chế nào và có giải pháp thay thế nào không?

Một hạn chế của DNS64/NAT64 là nó không hoạt động đối với các ứng dụng sử dụng trực tiếp địa chỉ IPv4 thay vì tên miền, vì DNS64 không thể can thiệp để chuyển đổi. Một giải pháp thay thế được đề cập là 464XLAT, tuy nhiên, một số hệ điều hành như Windows không hỗ trợ tính năng CLAT (Customer-Side Translator) là một thành phần của 464XLAT, làm cho nó khó áp dụng cho môi trường mạng doanh nghiệp và trung tâm dữ liệu.

PHẦN 2 – THỰC HÀNH

CHƯƠNG 10

HƯỚNG DẪN KIỂM TRA VÀ ĐÁNH GIÁ KẾT QUẢ TRIỂN KHAI IPv6 VÀ IPv6 ONLY

Sau khi hoàn tất các bước triển khai IPv6 hoặc chuyển đổi sang IPv6 Only, việc kiểm tra và đánh giá kết quả là một bước không thể thiếu để đảm bảo hệ thống mạng hoạt động như mong muốn và đáp ứng đầy đủ các yêu cầu kỹ thuật. Chương này sẽ hướng dẫn bạn cách sử dụng các công cụ kiểm tra trực tuyến phổ biến và đặc biệt là ứng dụng i-SPEED do Trung tâm Internet Việt Nam (VNNIC) phát triển, giúp kiểm tra khả năng kết nối, đo lường hiệu suất mạng IPv6, đồng thời phát hiện các vấn đề tiềm ẩn. Việc đo kiểm không chỉ giúp xác định hạ tầng mạng có hỗ trợ IPv6 hoàn chỉnh hay chưa, mà còn đánh giá tính sẵn sàng của các dịch vụ cung cấp ra bên ngoài.

10.1. CÁC NỘI DUNG CẦN KIỂM TRA, ĐÁNH GIÁ

Ngoài việc kiểm tra hoạt động của hệ thống sau khi khai báo như đã giới thiệu trong các bài LAB ở chương 8 và 9, nội dung kiểm tra và đánh giá ở chương này khẳng định ba câu hỏi quan trọng: Hạ tầng mạng của bạn đã sẵn sàng hoạt động với IPv6; dịch vụ cung cấp ra bên ngoài, như Website hay Email Server, có hỗ trợ IPv6 và làm sao mọi người biết Website của bạn đã sẵn sàng với IPv6? Chương này sẽ hướng dẫn bạn từng bước 3 nội dung chính như sau:

Kiểm tra hạ tầng mạng sẵn sàng với IPv6

Để đảm bảo hạ tầng mạng sẵn sàng hoạt động với IPv6, cần kiểm tra kết nối IPv6 từ các thiết bị đầu cuối như máy tính hoặc điện thoại. Các công cụ kiểm tra IPv6 trực tuyến như test-ipv6.com và ipv6-test.com sẽ giúp xác định khả năng kết nối IPv6 của thiết bị đã sẵn sàng.

Kiểm tra dịch vụ cung cấp ra bên ngoài đã hoạt động với IPv6

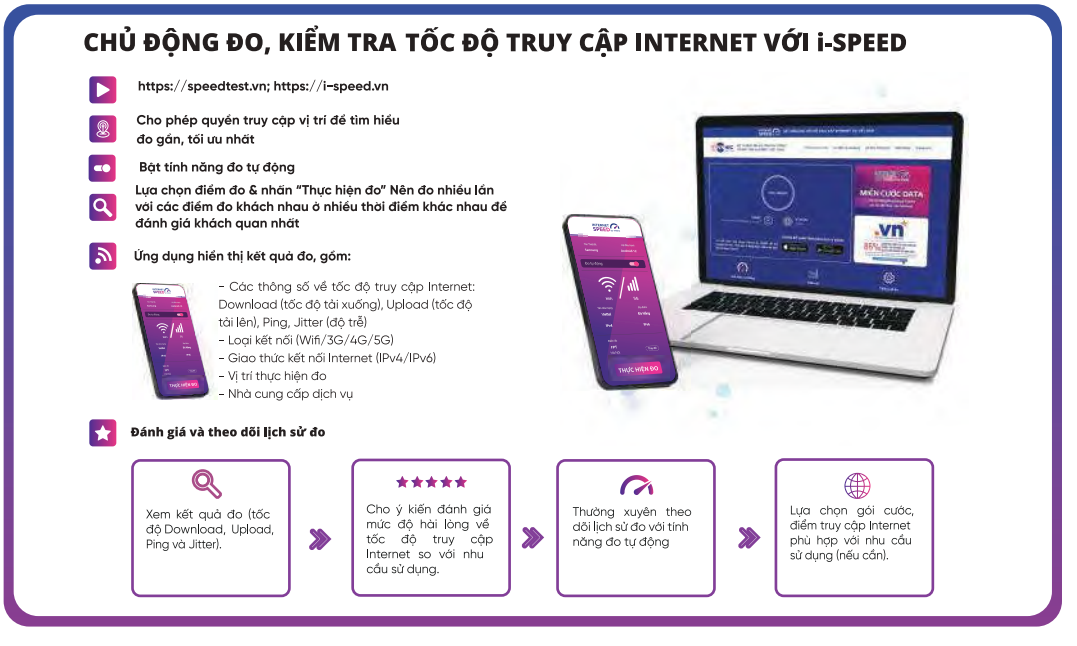
Cần sử dụng các công cụ để kiểm tra, bảo đảm chắc chắn các máy chủ dịch vụ do doanh nghiệp, cơ quan, tổ chức cung cấp ra bên ngoài đã hỗ trợ và hoạt động tốt với IPv6.

Hướng dẫn gắn logo "IPv6 Ready" cho Website

Logo "IPv6 Ready" là chứng nhận cho thấy Website của bạn hỗ trợ IPv6 một cách đầy đủ. Việc gắn Logo này không chỉ tăng uy tín cho Website mà còn thể hiện sự sẵn sàng và đóng góp cho tương lai của Internet. Chương này sẽ hướng dẫn bạn các bước để đạt được chứng nhận và tích hợp Logo lên Website. Thông qua Logo, người dùng có thể tự kiểm tra Website của bạn đã sẵn sàng với IPv6 hay chưa.

10.2 TỔNG QUAN VỀ ỨNG DỤNG I-SPEED BY VNNIC

Để kiểm tra và đánh giá chất lượng kết nối của hệ thống bạn cần đến một công cụ chuyên dụng và hiệu quả. Hiện nay có khá nhiều công cụ hữu ích nhưng tại Việt Nam, có một công cụ đa tính năng và miễn phí là i-SPEED – ứng dụng đo tốc độ mạng do Trung tâm Internet Việt Nam (VNNIC) phát triển, trực thuộc Bộ Khoa học và Công nghệ. i-SPEED không chỉ giúp bạn đo tốc độ tải xuống, tải lên, hay độ trễ (Ping, Jitter), mà còn kiểm tra xem mạng của bạn có đang sẵn sàng hoạt động IPv6 hay không. Điều tuyệt vời là i-SPEED hoàn toàn miễn phí, không tốn dữ liệu khi bạn đo kiểm thông qua mạng 4G/5G tại Việt Nam và cho kết quả rất trung thực, khách quan.



Hình 164. Giới thiệu về i-Speed by VNNIC

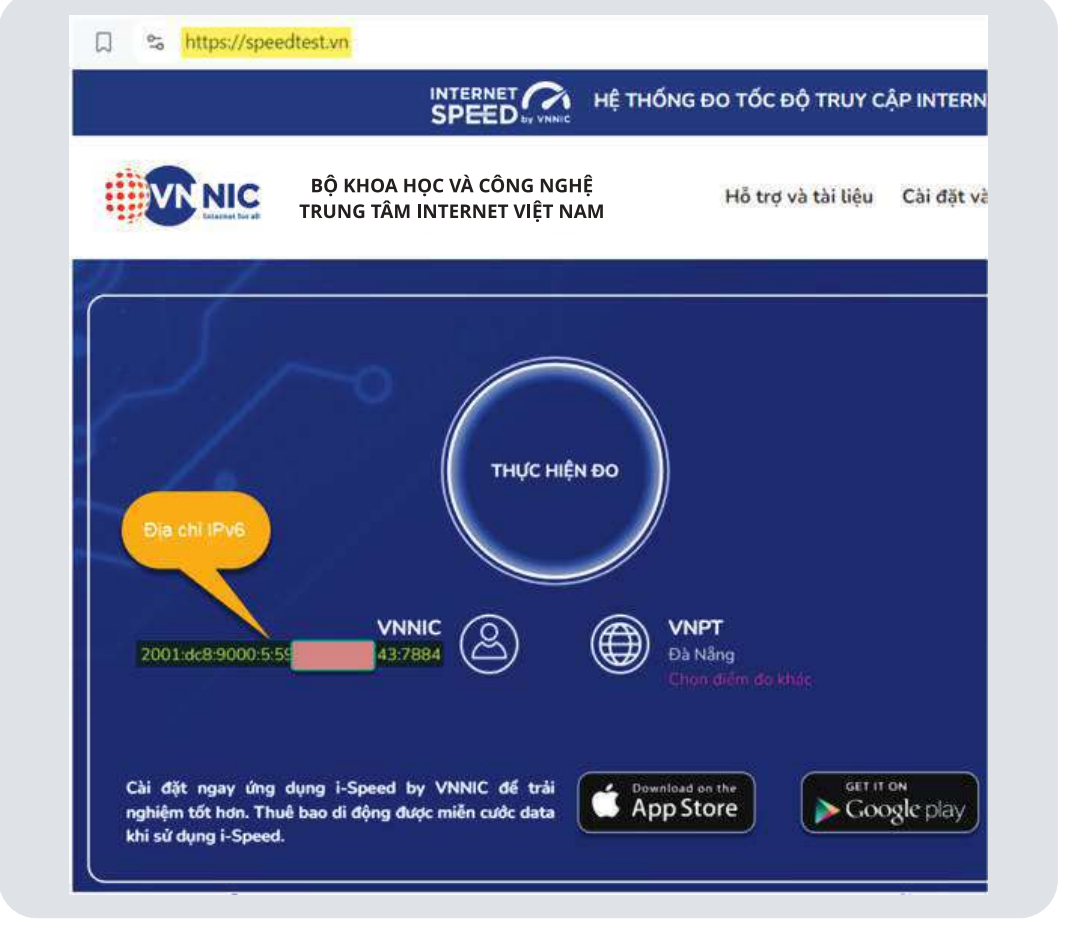
Bạn có thể tải i-SPEED trên Google Play (cho Android) hoặc App Store (cho iOS) bằng cách tìm "i-SPEED by VNNIC". Nếu không muốn cài ứng dụng, bạn cũng có thể truy cập trực tiếp qua web tại speedtest.vn để đo ngay trên trình duyệt. Chỉ với vài thao tác đơn giản, i-SPEED sẽ cho bạn cái nhìn rõ ràng về hiệu suất mạng IPv6, từ đó giúp bạn tự tin hơn khi kiểm tra hạ tầng mạng hay dịch vụ của mình. Trong các phần tiếp theo, chúng tôi sẽ hướng dẫn bạn cách dùng i-SPEED cùng các công cụ khác để kiểm tra từng khía cạnh của hệ thống IPv6 – từ hạ tầng nội bộ đến dịch vụ bên ngoài.

10.3 KIỂM TRA, ĐÁNH GIÁ HẠ TẦNG MẠNG ĐÃ SẴN SÀNG VỚI IPv6

Bước đầu tiên sau khi triển khai IPv6 là kiểm tra xem hạ tầng mạng đã sẵn sàng hoạt động với IPv6 hay chưa. Chúng ta có thể dùng các trang web trực tuyến hoặc ứng dụng i-Speed để thực hiện việc này. Sau đây là các cách để kiểm tra.

10.3.1 Sử dụng trang: speedtest.vn

Khi truy cập vào địa chỉ https://speedtest.vn/ bạn sẽ thấy cửa sổ bên dưới. Dù chưa bắt đầu đo nhưng nếu hệ thống mạng của bạn đã sẵn sàng với IPv6 thì trang web sẽ hiển thị địa chỉ IPv6. Bạn nhấp vào thực hiện đo để đo kiểm tốc độ Internet hệ thống mạng của cơ quan hay tốc độ Internet của nhà bạn. Bạn có để chọn điểm đo khác nếu muốn.



Hình 165. Kiểm tra trên máy tính, trường hợp mạng hỗ trợ IPv6

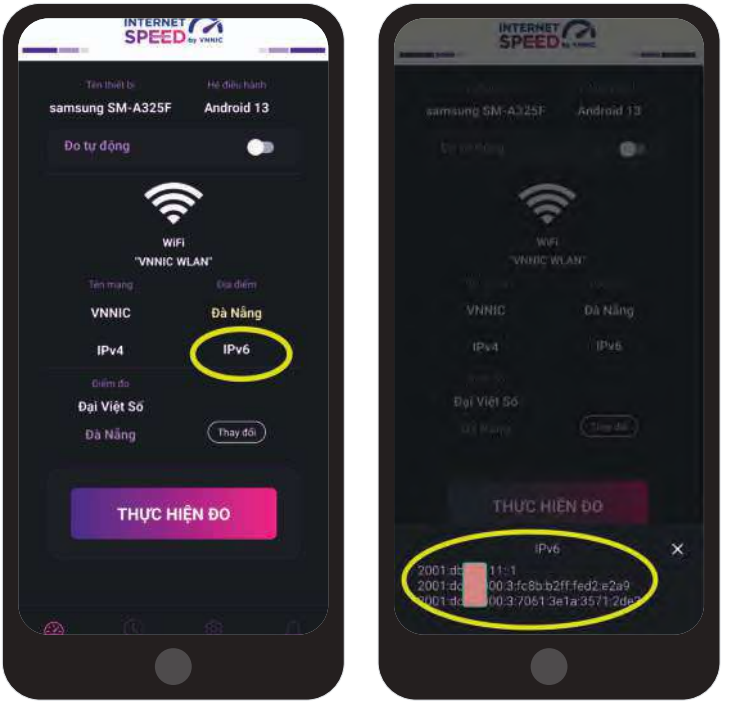
Nếu hệ thống mạng không hỗ trợ IPv6 thì khi truy cập địa chỉ trên bạn chỉ thấy địa chỉ IPv4. Dưới đây là kết quả của mạng (hoặc thiết bị) chỉ hỗ trợ IPv4, kết quả kiểm tra trên điện thoại di động.

Hình 166. Kiểm tra trên điện thoại, trường hợp mạng không hỗ trợ IPv6

10.3.2 Sử dụng ứng dụng i-Speed by VNNIC

Trường hợp này bạn sẽ sử dụng công cụ khác của VNNIC là ứng dụng i-Speed, giao diện sử dụng có khác một chút so với trang speedtest.vn nhưng cách thức kiểm tra cũng rất đơn giản và thuận tiện.

Sau khi mở ứng dụng, bạn sẽ thấy 2 biểu tượng IPv4 và IPv6. Nếu biểu tượng nào sáng lên thì hệ thống mạng hiện tại tại đó có hỗ trợ IPv4 và IPv6, nếu bị mờ có nghĩa ngược lại.



Hình 167. Cách kiểm tra hỗ trợ IPv6 bằng ứng dụng i-Speeed.

Để chắc chắn hệ thống mạng có hỗ trợ, bạn có thực hiện thêm một động tác nữa là nhấp vào biểu tượng IPv6 và sẽ thấy xuất hiện thông tin địa chỉ trên giao diện của ứng dụng. Sau đó bạn nhấp vào thực hiện đo và kiểm tra các thông số liên quan đến tốc độ và chất lượng kết nối Internet từ điện thoại của bạn. Bạn cũng có thể chọn các điểm đo khác nhau để đánh giá.

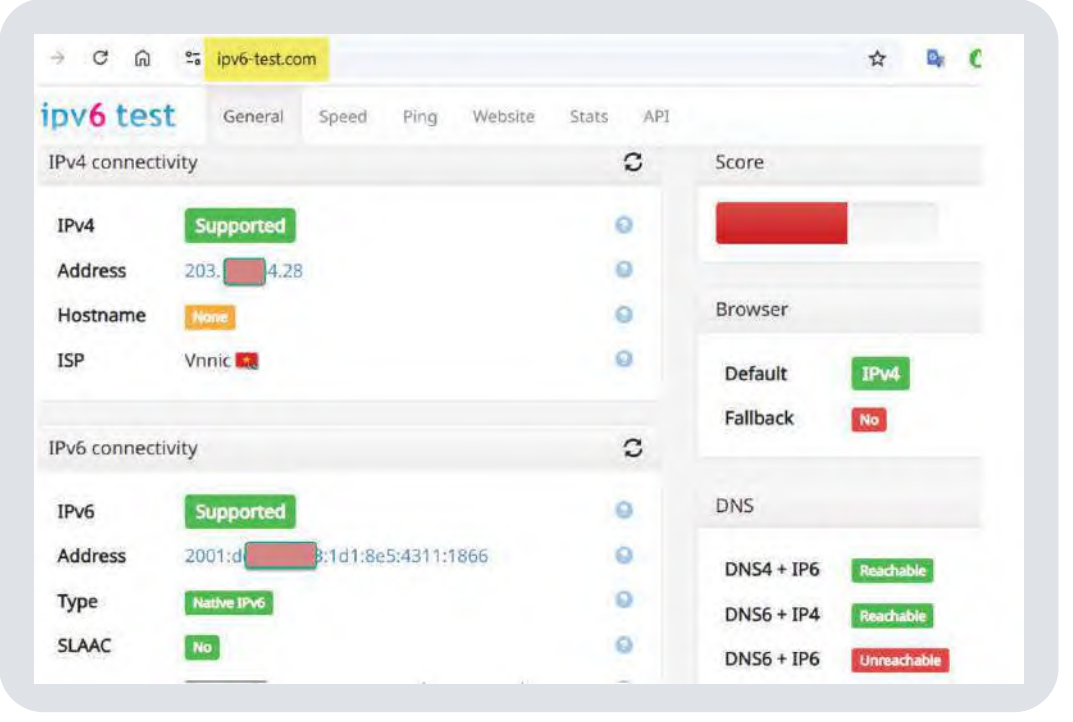
10.3.3 Sử dụng trang: test-ipv6.com

Đây là trang web của nước ngoài hỗ trợ kiểm tra kết nối của bạn tới trang web này đã hoạt động tốt với IPv6 hay chưa. Nếu bạn sử dụng Dual Stack thì trang web cho biết cả thông tin địa chỉ IPv4 và IPv6 mà mạng đang sử dụng để kết nối Internet. Trang web này chỉ kiểm tra kết nối của bạn đã hoạt động với IPv6 hay chưa chứ không thể thực hiện đo kiểm tốc độ như trang speedtest.vn.

Hình 168. Cách kiểm tra hỗ trợ IPv6 tại test-ipv6.com

10.3.4 Sử dụng trang: ipv6-test.com

Đây cũng là trang web của nước ngoài hỗ trợ kiểm tra IPv6 cho kết nối Internet của bạn tới trang web này, kết quả cũng tương tự như trang test-ipv6.com.



Hình 169. Cách kiểm tra hỗ trợ IPv6 tại ipv6-test.com

10.4 KIỂM TRA DỊCH VỤ CUNG CẤP RA BÊN NGOÀI HOẠT ĐỘNG VỚI IPv6

Sau khi khai báo cho các máy chủ dịch vụ của bạn hoạt động với IPv6, bạn cần thực hiện kiểm tra và đánh giá hoạt động. Dưới đây là hướng dẫn một số cách để giúp bạn kiểm tra.

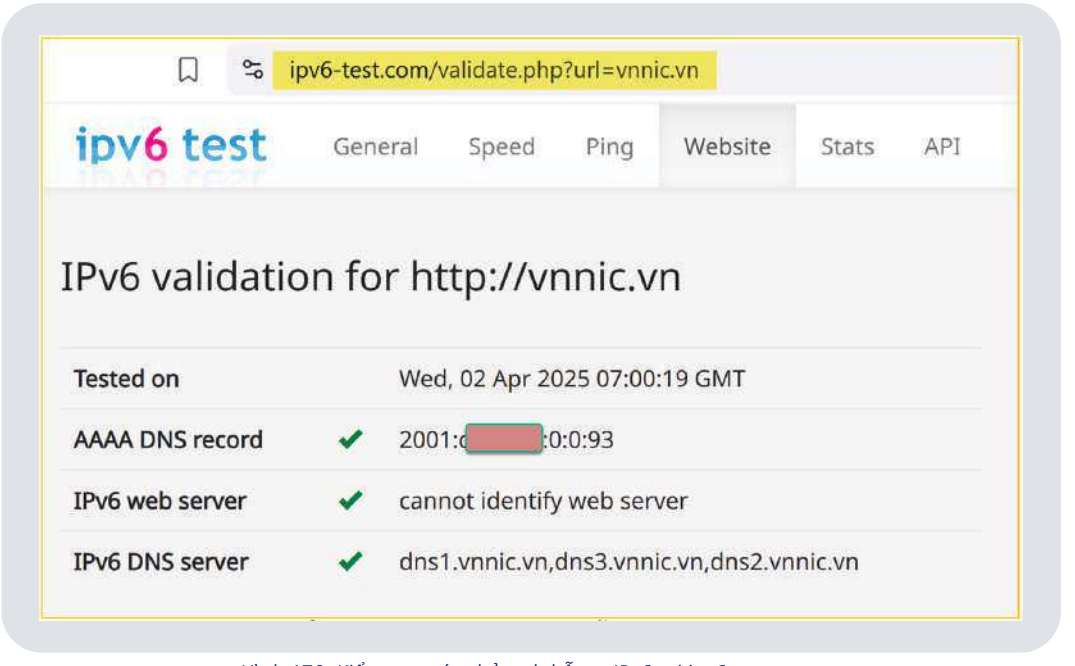
10.4.1 Kiểm tra bằng trang ipv6-test.com

Trang này hỗ trợ rất tốt trong việc kiểm tra máy chủ web đã sẵn sàng và hoạt động tốt với IPv6. Trang web này không cho bạn nhập địa chỉ URL của trang web mà bạn sử dụng liên kết theo cấu trúc sau:

https://ipv6-test.com/validate.php?url=Tên_Trang_Web

Bạn cần điền tên URL của trang cần kiểm tra vào phần cuối của cấu trúc trên. Giả sử bạn cần kiểm tra trang web có địa chỉ vnnic.vn đã sẵn sàng hoạt động với IPv6 thì bạn dùng liên kết:
https://ipv6-test.com/validate.php?url=vnnic.vn.

Kết quả sẽ như hình sau:

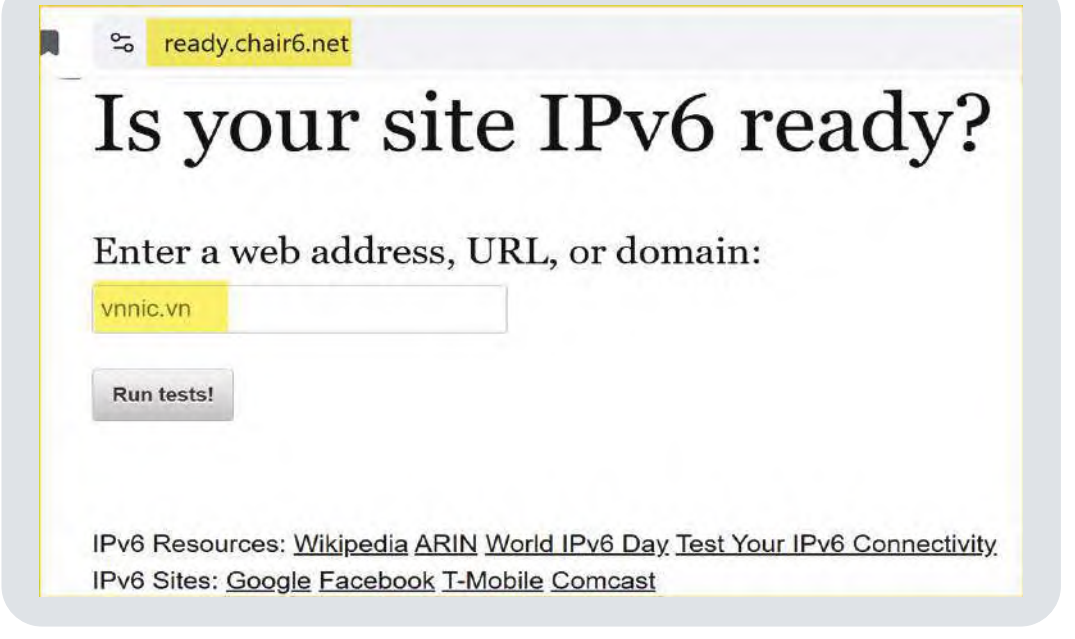


Hình 170. Kiểm tra máy chủ web hỗ trợ IPv6 tại ipv6-test.com

Các thông tin kiểm tra gồm máy chủ đã có bản ghi AAAA khai báo trên các DNS Server hay chưa, địa chỉ IPv6 của máy chủ này là gì và các DNS Server đã hoạt động với IPv6 hay chưa.

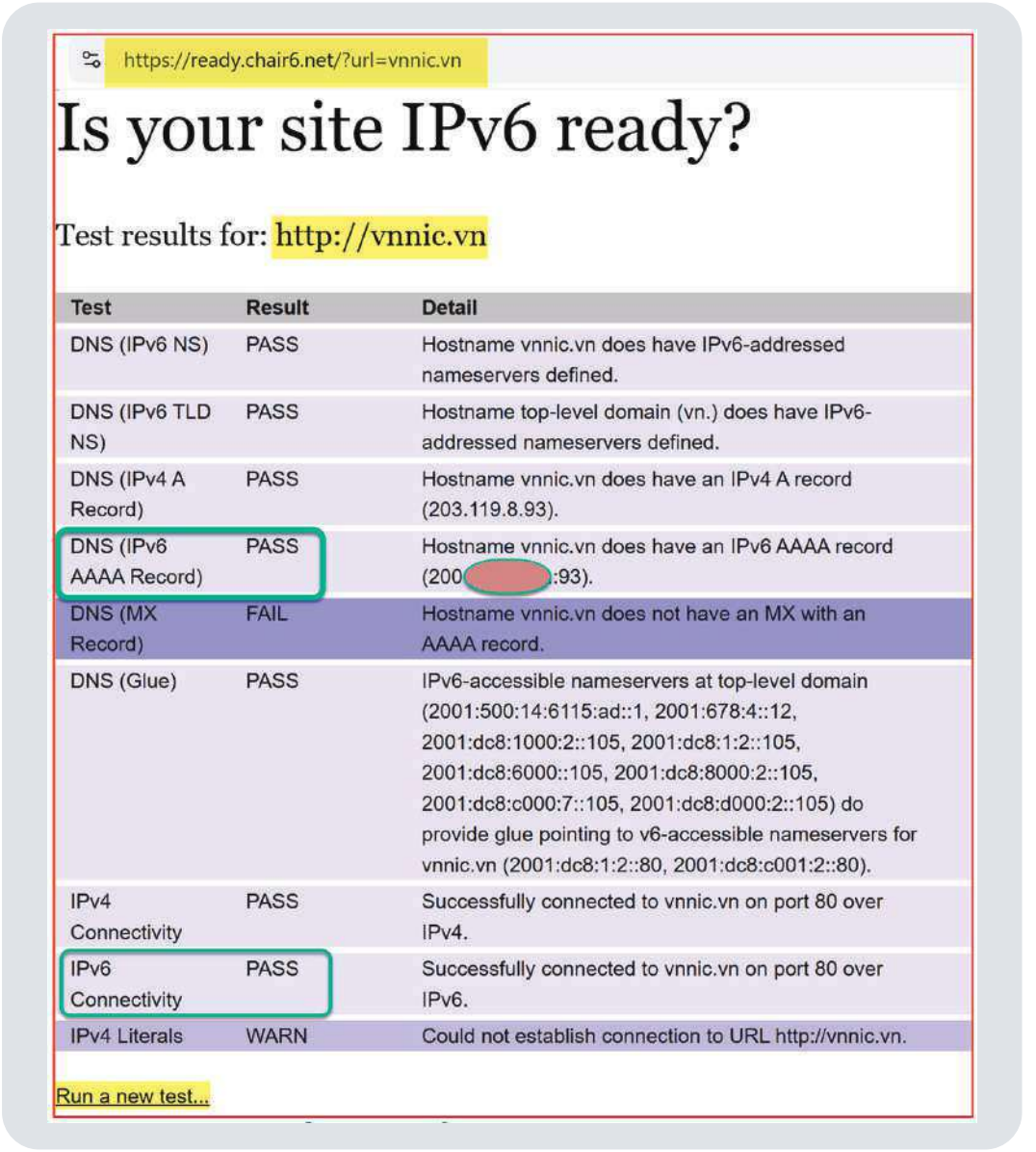
10.4.2 Kiểm tra bằng trang: ready.chair6.net

Trang web này cũng có tác dụng như trang web trên, cho phép kiểm tra máy chủ web của bạn đã sẵn sàng hoạt động với IPv6, nhưng điểm khác biệt là trang này cho phép bạn nhập trực tiếp địa chỉ URL cần kiểm tra thay vì nhập vào một liên kết. Giao diện chính của trang này như hình sau, bạn nhập địa chỉ URL và nhấp Run tests.



Hình 171. Giao diện của trang ready.chair6.net

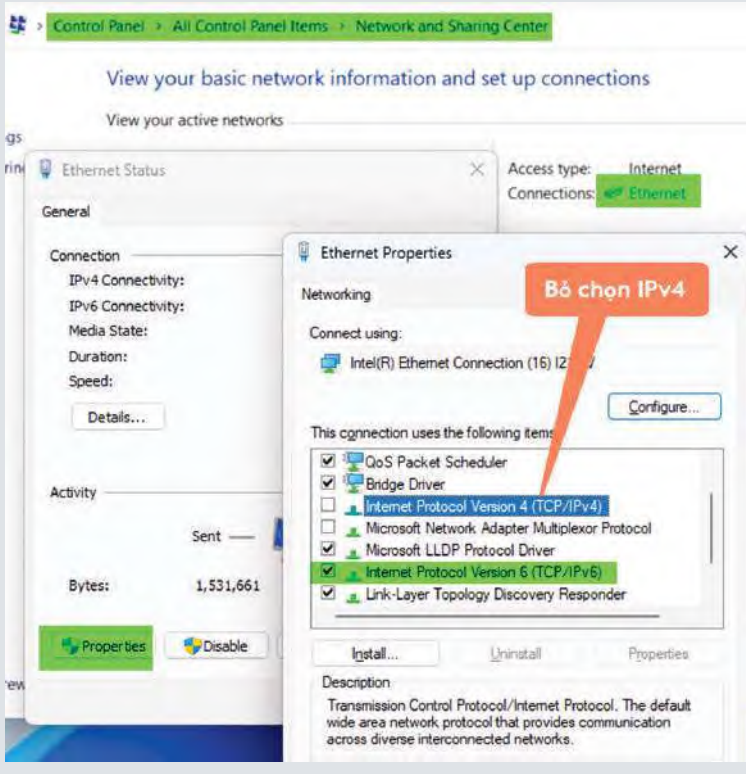
Nội dung kiểm tra như hình dưới, khá nhiều thông tin nhưng bạn chỉ cần chú ý 2 thông tin chính là AAAA Record và IPv6 Connectivity ở trạng thái PASS thì có nghĩa máy chủ web của bạn đã sẵn sàng hoạt động với IPv6.



Hình 172. Kết quả kiểm tra từ trang ready.chair6.net

10.4.3 Kiểm tra bằng máy tính IPv6 Only

Ở cách này chúng ta sẽ sử dụng một máy tính khai báo chỉ một mình giao thức IPv6 (từ một mạng đã sẵn sàng với IPv6) để kiểm tra các máy chủ cung cấp dịch vụ mà bạn cần kiểm tra. Với cách này bạn có thể kiểm tra tất cả các loại dịch vụ, không chỉ dịch vụ web như cách ở trên, nên cách này sẽ kiểm tra triệt để và chắc chắn hơn. Dưới đây là minh họa sử dụng máy tính Windows để kiểm tra.



Hình 173. Khai báo IPv6 Only cho máy tính thực hiện kiểm tra

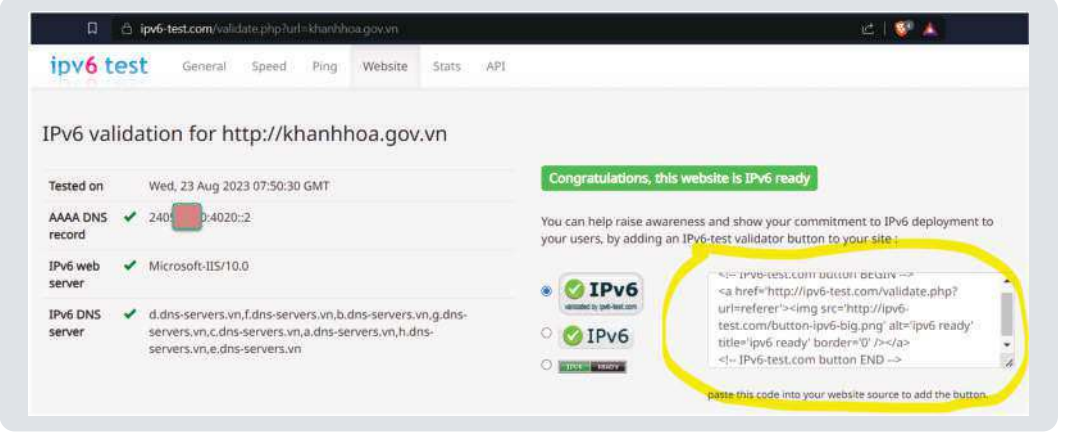
Sau khi khai báo chỉ sử dụng giao thức IPv6, bạn sẽ thực hiện kiểm tra dịch vụ của các máy chủ bạn cần kiểm tra để đánh giá dịch vụ đã hoạt động tốt với IPv6.

Hình 174. Kiểm tra máy chủ dịch vụ từ máy tính IPv6 Only

10.5 HƯỚNG DẪN GẮN LOGO "IPv6 READY" CHO WEBSITE

Sau khi xác nhận máy chủ web của bạn đã hỗ trợ IPv6, việc gắn logo "IPv6 Ready" lên Website là một bước quan trọng để chứng minh điều này với cộng đồng. Có nhiều phương pháp để thực hiện, nhưng dưới đây là cách đơn giản, nhanh chóng và hiệu quả, đồng thời cho phép người dùng kiểm tra và xác nhận Website của bạn đã hoạt động với IPv6.

Để thực hiện, bạn vẫn sử dụng trang ipv6-test.com, công cụ dùng để kiểm tra máy chủ dịch vụ như đã trình bày ở trên. Ví dụ, người quản trị viên của trang "Cổng thông tin điện tử tỉnh Khánh Hòa" muốn gắn logo IPv6 thì người đó cần dùng liên kết https://ipv6-test.com/validate.php?url=khanhhoa.gov.vn để kiểm tra mức độ sẵn sàng của máy chủ.



Hình 175. Kiểm tra máy chủ dịch vụ khanhhoa.gov.vn

Trong kết quả kiểm tra, bạn sẽ thấy một đoạn mã Script ở phía bên phải màn hình. Đoạn mã này cho phép bạn thêm logo "IPv6 Ready" lên Website. Bạn có thể chọn một trong ba mẫu logo, sao chép đoạn Script tương ứng, rồi dán vào các trang trên Website để hiển thị logo. Vị trí đặt logo trên Website tùy thuộc vào ý muốn của bạn.

Hình 176. Logo IPv6 Ready do ipv6-test.com cung cấp

Kết quả là Website của bạn sẽ hiển thị logo "IPv6 Ready" do ipv6-test.com cung cấp. Nếu người dùng muốn kiểm tra xem Website của bạn đã sẵn sàng với IPv6 hay chưa thì họ chỉ cần nhấp vào logo đó. Thao tác này sẽ dẫn họ đến trang https://ipv6-test.com/validate.php?url=khanhhoa.gov.vn, nơi hiển thị thông tin xác nhận máy chủ web của bạn đã hỗ trợ IPv6 như đã đề cập.

Đây là một phương pháp đơn giản nhưng rất hiệu quả. Người dùng có thể dễ dàng kiểm tra Website của bạn, qua đó nâng cao uy tín và độ tin cậy cho trang web.

10.6 TỔNG KẾT CHƯƠNG 10

Chương 10 đã cung cấp cái nhìn toàn diện về quy trình kiểm tra và đánh giá sau khi triển khai IPv6 hoặc chuyển đổi sang mô hình IPv6 Only. Đây là bước quan trọng để đảm bảo hệ thống mạng hoạt động ổn định, đáp ứng các tiêu chuẩn kỹ thuật và sẵn sàng cung cấp dịch vụ ra bên ngoài.

Các nội dung trọng tâm của chương bao gồm:

- **Kiểm tra hạ tầng mạng nội bộ:** Sử dụng các công cụ như test-ipv6.com, ipv6-test.com, speedtest.vn và ứng dụng i-SPEED by VNNIC để xác định khả năng kết nối và hiệu suất mạng IPv6 từ thiết bị đầu cuối. Việc này giúp xác nhận hạ tầng đã sẵn sàng với IPv6.
- **Đánh giá dịch vụ cung cấp ra bên ngoài:** Hướng dẫn cách kiểm tra các máy chủ dịch vụ (Web, Email...) đã hoạt động tốt với IPv6 chưa, thông qua các công cụ như ipv6-test.com, ready.chair6.net, hoặc thực hiện kiểm tra trực tiếp bằng máy tính cấu hình IPv6 Only.
- **Gắn logo "IPv6 Ready":** Giới thiệu cách hiển thị chứng nhận "IPv6 Ready" lên Website, không chỉ giúp nâng cao uy tín mà còn tạo điều kiện để người dùng xác minh tính sẵn sàng với IPv6 một cách trực quan.

Chương này nhấn mạnh vai trò của việc đo kiểm như một phần không thể thiếu trong toàn bộ quá trình triển khai IPv6, giúp người quản trị hệ thống kịp thời phát hiện và xử lý các vấn đề, đồng thời nâng cao độ tin cậy của dịch vụ trên môi trường Internet mới. Qua đó, chương cũng khuyến khích các tổ chức ứng dụng và phổ biến IPv6 rộng rãi hơn trong thực tiễn.

10.7 CÂU HỎI ÔN TẬP CHƯƠNG 10

01

Kiểm tra và đánh giá kết quả triển khai IPv6 là gì?

Sau khi triển khai IPv6 hoặc chuyển đổi sang mô hình IPv6 Only, kiểm tra và đánh giá là bước quan trọng để đảm bảo hệ thống mạng hoạt động đúng như mong đợi và đáp ứng các yêu cầu kỹ thuật. Quá trình này bao gồm kiểm tra khả năng kết nối, đo lường hiệu suất mạng IPv6 và phát hiện các vấn đề tiềm ẩn, giúp xác định hạ tầng mạng có hỗ trợ IPv6 hoàn chỉnh hay không và đánh giá sự sẵn sàng của các dịch vụ cung cấp ra bên ngoài.

02

Những nội dung chính cần kiểm tra và đánh giá sau khi triển khai IPv6 là gì?

Các nội dung chính cần kiểm tra và đánh giá bao gồm:

- Kiểm tra hạ tầng mạng nội bộ đã sẵn sàng hoạt động với IPv6.
- Kiểm tra các dịch vụ cung cấp ra bên ngoài (như Website, Email Server) đã hỗ trợ và hoạt động tốt với IPv6.
- Hướng dẫn cách gắn logo "IPv6 Ready" cho Website để thông báo về sự sẵn sàng với IPv6.

03

Làm thế nào để kiểm tra hạ tầng mạng nội bộ đã sẵn sàng với IPv6?

Có thể sử dụng các công cụ trực tuyến hoặc ứng dụng để kiểm tra hạ tầng mạng nội bộ:

- **Sử dụng trang web:** Truy cập các trang như speedtest.vn, test-ipv6.com, hoặc ipv6-test.com. Các trang này sẽ hiển thị địa chỉ IP (IPv4 hoặc IPv6) mà mạng của bạn đang sử dụng để kết nối Internet, hoặc báo cáo mức độ hỗ trợ IPv6.
- **Sử dụng ứng dụng i-SPEED by VNNIC:** Ứng dụng này không chỉ đo tốc độ mạng mà còn kiểm tra khả năng hỗ trợ IPv6 của kết nối hiện tại. Biểu tượng IPv6 sẽ sáng lên nếu mạng có hỗ trợ.

04

Công cụ nào giúp kiểm tra dịch vụ cung cấp ra bên ngoài đã hoạt động với IPv6?

Để kiểm tra các máy chủ dịch vụ (Web, Email...) đã hỗ trợ IPv6, có thể sử dụng các công cụ sau:

- Trang ipv6-test.com: Sử dụng liên kết cấu trúc https://ipv6-test.com/validate.php?url=Tên_Trang_Web để kiểm tra máy chủ web, bao gồm kiểm tra bản ghi AAAA, địa chỉ IPv6 của máy chủ và sự hoạt động của DNS Server với IPv6.
- Trang ready.chair6.net: Cho phép nhập trực tiếp địa chỉ URL để kiểm tra sự sẵn sàng của máy chủ web với IPv6, chú trọng các thông tin như AAAA Record và IPv6 Connectivity.
- Kiểm tra bằng máy tính IPv6 Only: Cấu hình một máy tính chỉ sử dụng giao thức IPv6 để kiểm tra triệt để tất cả các loại dịch vụ mà không chỉ giới hạn ở dịch vụ web.

05

Ứng dụng i-SPEED by VNNIC là gì và có tác dụng gì trong việc kiểm tra IPv6?

i-SPEED là ứng dụng đo tốc độ mạng do Trung tâm Internet Việt Nam (VNNIC) phát triển. Ngoài chức năng đo tốc độ tải xuống, tải lên và độ trễ, i-SPEED còn tích hợp tính năng kiểm tra xem mạng hiện tại có hỗ trợ hoạt động với IPv6 hay không. Ứng dụng này miễn phí và cho kết quả khách quan, có thể tải về trên thiết bị di động hoặc truy cập trực tiếp qua trang web speedtest.vn.

06

Gắn Logo "IPv6 Ready" cho Website có ý nghĩa gì?

Gắn logo "IPv6 Ready" cho Website là cách chứng nhận rằng Website đã hỗ trợ IPv6 một cách đầy đủ. Việc này không chỉ giúp tăng uy tín cho Website mà còn thể hiện sự sẵn sàng và đóng góp vào sự phát triển của Internet tương lai. Logo này cũng giúp người dùng dễ dàng xác minh Website có hỗ trợ IPv6 hay không chỉ bằng cách nhấp vào nó.

07

Làm thế nào để gắn Logo "IPv6 Ready" cho Website?

Cách đơn giản và hiệu quả để gắn logo "IPv6 Ready" là sử dụng trang ipv6-test.com. Sau khi kiểm tra sự sẵn sàng của Website với IPv6 bằng công cụ này, trang web sẽ cung cấp một đoạn mã Script. Người quản trị viên chỉ cần sao chép đoạn mã tương ứng với mẫu logo mong muốn và dán vào các trang trên Website. Khi người dùng nhấp vào logo, họ sẽ được dẫn đến trang xác nhận trên ipv6-test.com.

08

Tại sao việc đo kiểm sau khi triển khai IPv6 lại quan trọng?

Việc đo kiểm sau khi triển khai IPv6 là vô cùng quan trọng vì nó giúp:

- Đảm bảo hệ thống mạng hoạt động ổn định và đáp ứng các tiêu chuẩn kỹ thuật.
- Xác định chính xác hạ tầng mạng đã sẵn sàng hoạt động với IPv6 hoàn chỉnh hay chưa.
- Đánh giá tính sẵn sàng và hoạt động tốt của các dịch vụ cung cấp ra bên ngoài trên nền tảng IPv6.
- Kịp thời phát hiện và xử lý các vấn đề phát sinh trong quá trình triển khai, từ đó nâng cao độ tin cậy của dịch vụ trên môi trường Internet mới.

PHỤ LỤC

1. CÁC RFC PHỔ BIẾN VỀ IPv6

Dưới đây là danh sách các RFC quan trọng nhất liên quan đến IPv6, giúp bạn dễ dàng tra cứu và hiểu rõ hơn về cấu trúc, giao thức, công nghệ chuyển đổi và các dịch vụ mạng của giao thức IPv6. Chi tiết danh sách các RFC về IPv6 được liệt kê tại trang web: https://www.system.de/ipv6-rfc/.

Tên RFC	Tiêu đề	Năm phát hành	Danh mục	Mô tả	Cập nhật/ thay thế cho
RFC 8200	Internet Protocol, Version 6 (IPv6) Specification	2017	Cấu trúc địa chỉ	Định nghĩa cấu trúc gói IPv6, các trường trong header và tính năng cơ bản của IPv6.	Thay thế RFC 2460
RFC 4291	IP Version 6 Addressing Architecture	2006	Cấu trúc địa chỉ	Mô tả cấu trúc địa chỉ IPv6, bao gồm unicast, multicast, anycast và định dạng 128 bit.	Cập nhật bởi RFC 5952
RFC 4193	Unique Local IPv6 Unicast Addresses	2005	Cấu trúc địa chỉ	Định nghĩa địa chỉ ULA dành cho mạng nội bộ, không định tuyến trên Internet.	Không
RFC 4007	IPv6 Scoped Address Architecture	2005	Cấu trúc địa chỉ	Mô tả kiến trúc địa chỉ có phạm vi (link-local, site-local) trong IPv6.	Không
RFC 4861	Neighbor Discovery for IP version 6 (IPv6)	2007	Giao thức hỗ trợ	Định nghĩa giao thức Neighbor Discovery, hỗ trợ phát hiện địa chỉ, cấu hình tự động và quản lý mạng.	Thay thế RFC 2461
RFC 4862	IPv6 Stateless Address Autoconfiguration	2007	Giao thức hỗ trợ	Định nghĩa cơ chế SLAAC cho phép thiết bị tự động cấu hình địa chỉ IPv6 mà không cần DHCP.	Thay thế RFC 2462
RFC 4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	2005	Công nghệ chuyển đổi	Mô tả các cơ chế chuyển đổi như Dual Stack và Tunneling (6in4) từ IPv4 sang IPv6.	Thay thế RFC 2893
RFC 3056	Connection of IPv6 Domains via IPv4 Clouds	2001	Công nghệ chuyển đổi	Mô tả kỹ thuật 6to4 cho phép kết nối mạng IPv6 thông qua hạ tầng IPv4.	Không
RFC 6146	Stateful NAT64: Network Address and Protocol Translation	2011	Công nghệ chuyển đổi	Định nghĩa NAT64 để chuyển đổi từ client IPv6 sang server IPv4, giúp giao tiếp giữa hai mạng.	Không
RFC 6147	DNS64: DNS Extensions for Network Address Translation	2011	Công nghệ chuyển đổi	Mô tả DNS64, cho phép NAT64 hoạt động bằng cách tạo bản ghi AAAA từ bản ghi A, hỗ trợ ánh xạ địa chỉ.	Không
RFC 4038	Application Aspects of IPv6 Transition	2005	Dịch vụ mạng	Hướng dẫn triển khai IPv6 trong các ứng dụng (web, email...) nhằm đảm bảo tính tương thích với IPv4.	Không
RFC 4941	Privacy Extensions for Stateless Address Autoconfiguration	2007	Dịch vụ mạng	Đề xuất cơ chế tạo địa chỉ IPv6 tạm thời nhằm bảo vệ quyền riêng tư của người dùng khi sử dụng SLAAC.	Không

Tên RFC	Tiêu đề	Năm phát hành	Danh mục	Mô tả	Cập nhật/ thay thế cho
RFC 4443	Internet Control Message Protocol (ICMPv6) for IPv6	2006	Dịch vụ mạng	Định nghĩa ICMPv6, giao thức quản lý và báo lỗi trong IPv6, giúp xử lý các thông báo lỗi và kiểm tra kết nối.	Thay thế RFC 2463
RFC 3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	2004	Dịch vụ mạng	Mô tả giao thức MLDv2, hỗ trợ quản lý nhóm multicast trong IPv6, thay thế phiên bản trước đó.	Thay thế RFC 2710

Bảng 16. Danh sách những RFC phổ biến nhất liên quan đến IPv6

2. TÀI LIỆU THAM KHẢO

Dưới đây là một số sách tham khảo về IPv6:

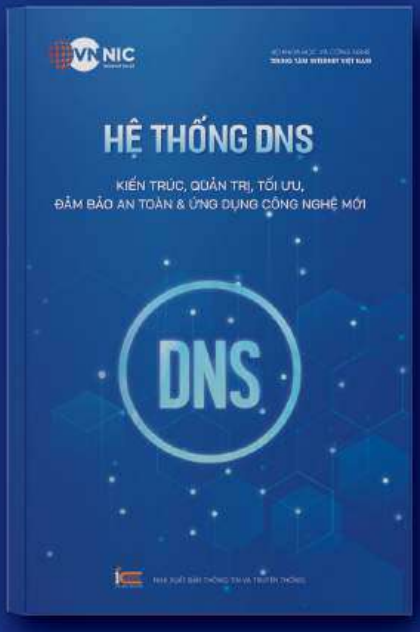
- **Coffey, T. (2017).** IPv6 Address Planning: Designing the Future of Your Network. Cisco Press.
- **Barton, R. (2020).** BRKIP6-2223 – IPv6 for the world of IoT [Conference presentation]. Cisco Live. *https://www.ciscolive.com/*
- **ETSI Industry Specification Group (ISG) IPv6 Integration. (2020).** IPv6 best practices, benefits, transition challenges and the way forward *https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp35_IPv6_Best_Practices_Benefits_Transition_Challenges_and_the_Way_Forward.pdf*
- **ETSI Industry Specification Group (ISG) IPv6 Integration. (2018).** *IPv6-based 5G mobile wireless internet* (ETSI GR IP6 011 V1.1.1). European Telecommunications Standards Institute. *https://www.etsi.org/deliver/etsi_gr/IP6/001_099/011/01.01.01_60/gr_ip6011v010101p.pdf*
- **ETSI Industry Specification Group (ISG) IPv6 Integration. (2017)**. IPv6 deployment in the enterprise (ETSI GR IP6 001 V1.1.1). European Telecommunications Standards Institute. *https://www.etsi.org/deliver/etsi_gr/IP6/001_099/001/01.01.01_60/gr_ip6001v010101p.pdf*
- **ETSI Industry Specification Group (ISG) IPv6 Integration. (2017).** IPv6-based Internet of Things (ETSI GR IP6 008 V1.1.1). European Telecommunications Standards Institute. *https://www.etsi.org/deliver/etsi_gr/IP6/001_099/008/01.01.01_60/gr_ip6008v010101p.pdf*
- **Hagen, S. (2002)**. IPv6 Essentials. O'Reilly Media. **Graziani, R. (2005)**. IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6. Cisco Press.
- **Li, Z. (2023).** IPv6 enhanced: A new era of IP networks for 5G and cloud [Conference presentation]. Huawei Technologies Co., Ltd. *https://www.ipv6plus.net/resources/IPv6_Plus/IPv6_Enhanced-A_New_Era_of_IP_Networks_for_5G_and_Cloud_2023.pdf*
- **Niall Richard Murphy, David Malone (2005)**. IPv6 Network Administration: Teaching Turtle to IPv6. (2002). O'Reilly Media.
- **Patrick Grossetete, Ciprian P. Popoviciu, Fred Wettling (2008)**. Global IPv6 Strategies: Business and Operational. (2004). Cisco Press.

VNNIC
Internet for all

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM INTERNET VIỆT NAM

MỘT SỐ CUỐN SÁCH TIÊU BIỂU KHÁC VỀ INTERNET VIỆT NAM

BÁO CÁO INTERNET,
TÀI NGUYÊN INTERNET
VIỆT NAM 2024



HỆ THỐNG DNS
KIẾN TRÚC, QUẢN TRỊ, TỐI ƯU,
ĐẢM BẢO AN TOÀN & ỨNG DỤNG
CÔNG NGHỆ MỚI

TRỤ SỞ TẠI TP. HÀ NỘI

Trụ sở chính: Tòa nhà VNTA, đường Dương Đình Nghệ, P. Yên Hòa, Q. Cầu Giấy, Hà Nội
Khu công nghệ cao Hòa Lạc, Thạch Thất, Hà Nội
Tel: 024 3556 4944 | Email: info@vnnic.vn | Website: https://vnnic.vn

CHI NHÁNH TẠI TP. ĐÀ NẴNG

Lô 21, Đường số 7, KCN An Đồn, Q. Sơn Trà, TP. Đà Nẵng

CHI NHÁNH TẠI TP. HỒ CHÍ MINH

Đường số 20 - Khu chế xuất Tân Thuận, Q. 7, TP. Hồ Chí Minh

SÁCH KHÔNG BÁN